Cornell University
IT Security Office

COMPUTER SECURITY AT CORNELL | *secure your computer on and off campus*

COMPUTER SECURITY AT CORNELL

secure your computer on and off campus

1. Why Secure Computing Is Your Responsibility 5
   - Consequences of Not Practicing Secure Computing 6
   - Cornell Policies 6

2. Recognizing and Responding to Security Issues 9
   - Possible Security Problems 9
   - Responding to a Security Problem 10
   - About the IT Security Office 11

3. Protecting Your Identity 13
   - NetID Password Theft 13
   - How to Create a Strong NetID Password 19
   - Best Practices for Managing Passwords Safely 21

4. Protecting University Data 24
   - Know What Information Is on Your Computer and Secure It 25
   - University Data Currently Classified as Confidential 26
   - Handling Sensitive Data 27
   - Consequences of Mishandling Sensitive Data 29
   - Why Data Security Is Important 30
   - Data Discovery Software 31

5. Securing Your Computer 34
   - Set a Strong Password for Access to the Computer 34
   - Keep Your Software Updated 35
   - Run Up-to-Date Antivirus Software 35
   - Enable Your Firewall 35
   - Set Your Screen to Lock Automatically 36
   - Turn Off Anonymous Access to Your Computer 36
   - Use a Less Privileged Account 37
   - Additional Requirements for Computers and Mobile Devices Storing Confidential Data . . . 37
   - Security Precautions for Mobile Devices 38

6. Internet Safety 41
   - What You Need to Know About Privacy and the Internet 41
   - How to Guard Against Internet Fraud 44
   - How Malware Gets on Your Computer 53
   - How to Enhance Your Web Browser's Security (Browser Hardening) 56

7. Working Off Campus 60
   - Working on Your Computer at Home 60
   - Away from Home and Work 62
   - Accessing Cornell Services from Other Computers 63

Introduction

It's 8:30 a.m. You sit down at your computer, ready to plow through the day's work. Today you have some can't-miss deadlines and you know you'll need most of the day to meet one of them. Your computer seems sluggish, so you restart it. Although it takes longer than usual, finally you're in. No – not really. You can't access your email or the web.

You've got a security problem. Your stomach sinks as you think back on everything you've done over the past few days. The university systems you've accessed. The database you just updated. Your email. How long has your computer been compromised? What information has the intruder accessed and what are they doing with it? Is more than just your information at stake?

Chances are one of your friends or colleagues, if not you, has had an experience like this one. It happens everywhere computers are connected to networks, at home, at corporations, at universities. It happens at Cornell.

This handbook explains, as simply as possible, why computer security is something everyone at Cornell needs to pay attention to, and what steps you can take to:

- Keep your NetID password from getting stolen
- Guard your computer against viruses, drive-by downloads, and other security threats
- Safeguard sensitive university data
- Outsmart cyber-scammers
- Avoid computer security risks at home and on the road
- Be a good network citizen, so your actions, or inaction, do not negatively affect others

Look for these updates in this 2011 edition of the ***Computer Security at Cornell*** handbook

- Many new quotes, sidebars, and vocabulary definitions
- All new "In the News" articles at the end of each chapter
- Information about the data discovery effort at Cornell
- An explanation of Extended Validation Certificates
- Links to updated documentation (Windows 7, Mac OS)
- Links to new resources
- More information about securing your mobile device (smart phone, tablet, etc...)

CHAPTER 1 Why Secure Computing Is Your Responsibility

It takes more than antivirus software to safeguard Cornell's computing resources and data. It takes you. Taking steps to secure your computer not only helps keep your data safe, it demonstrates your commitment to protecting the university network and all data created, stored, and shared over the network by the campus community.

While your department may have technical staff to provide computer setup and assistance, ultimately you are responsible for taking care of your computer and guarding the information it holds. Following security guidelines and good business practices is part of doing your job.

> *"The vast majority of computer breaches that we have investigated over the past few years have been the result of poor personal choices, weak computer practices, and less-than-satisfactory data handling procedures."*
>
> *Steve Schuster, Cornell Information Technologies*

Everyone has the responsibility to protect Cornell data on any computer used for Cornell work. Cornell data on your computer is university property that has been placed in your care.

Much of the data we work with is sensitive, such as Social Security numbers, payroll information, grades, and more. However, all university data needs to be protected. For more examples of sensitive data see Protecting University Data, page 24.

Chronology of Data Breaches

In 2010, there were 593 reported security breaches involving sensitive data, 73 of which happened at colleges and universities.

View a list of security breaches, including those reported in higher education, from 2005 to the present at www.privacyrights.org/data-breach.

Privacy Rights Clearinghouse

Consequences of Not Practicing Secure Computing

Keeping your computer secure takes vastly less time than recovering from a security problem. If your computer is compromised, you will likely lose access to it for at least a few hours, possibly days. You may also lose any work you did since your computer was last backed up.

If the security problem put sensitive data at risk, or if your computer is lost or stolen, the effects can be far-reaching:

- You may be held accountable for any negligent action, or inaction, that led to the incident.
- The university may suffer financial loss as well as loss of reputation.
- Any individual whose data is compromised could potentially also suffer financial loss, identity theft, and unwanted public exposure of private information.

Recovering from a computer compromise or loss of sensitive data, large or small, can take many people many hours and, as a result, is an expensive activity. For details on steps taken, and people involved to investigate an incident, see Consequences of Mishandling Sensitive Data, page 29.

Cornell Policies

At Cornell a wide range of university policies address the important issues surrounding computer security and data protection.

> *"Cornell's policies connect the university's mission to the everyday actions of its community, clarify the institution's expectations of its individual members, mitigate institutional risk, enhance efficiency, and support the university's compliance with laws and regulations."*
>
> *www.dfa.cornell.edu/treasurer/policyoffice*

These policies apply to all faculty, staff, and students. For more information, see Appendix II: An Overview of University Policies on Computer Security and Data Protection, page 68.

The university has requirements for maintaining the security of computers and the information they store. One of the goals of this handbook is to make it clear how these requirements apply to you. Detailed technical information is available in Policy 5.10, Information Security www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/informationtech/infosecurity.cfm.

"I use a Mac, so I don't have to worry about security problems."

Not true! Every kind of computer is vulnerable to security problems. See In the News: Updated rogue AV installs on Macs without password, page 8.

Whether you use a Macintosh or Windows computer makes no difference for one of the biggest security problems – loss or theft of your computer.

In the News:

Hackers hit universities' database 'jackpots'

Excerpts from the article by Sarah King Head, University World News
December 12, 2010

Since 2008, 158 data breaches have compromised more than 2.3 million records at American higher education institutions, according to a recent report by Application Security, Inc, a US database safety company. [Download the PDF report at www.appsecinc.com/techdocs/whitepapers/Higher-Ed-Whitepaper-Edited.pdf.]

Identity theft has become the US's largest consumer complaint, according to the Federal Trade Commission (FTC), with nearly a million new victims each year. The problem has been exacerbated – and the illicit rewards made greater – by cyber criminals successfully hacking into the databases of semi-autonomous tertiary educational institutions.

"When an attacker gets access to university databases, it's like hitting the jackpot," says Josh Shaul, the New York-based Application Security's vice-president of product management.

...College databases contain such an extensive range of personally identifiable information (PII), from key financial information to "credit card numbers, Social Security numbers, and the healthcare records of employees, students, parents and alumni."

For larger institutions, with tens of thousands of students along with staff and faculty, "a university or college could be housing potentially billions of PII [personally identifiable information]," says Shaul.

The recent data breach at the University of Central Missouri is one example where large amounts of data were successfully captured.

According to the Identity Theft Resource Center (ITRC) in San Diego, California, two students there generated a virus to gain remote access to data associated with more than 90,000 faculty, staff, alumni and students through university computer labs and the library.

They credited their own student accounts and changed their grades during the 2009 autumn term before being stopped in their tracks while attempting to sell the information to an undercover FBI agent for $35,000.

Similarly, in August a laptop containing the Social Security numbers of more than 10,000 applicants to the West Hartford campus of the University of Connecticut was stolen. Administrators have been conducting damage control ever since – contacting the compromised individuals and offering them credit-monitoring coverage for two years at the university's expense.

The $204 per compromised record that Poneman Institute estimates it costs to remedy a breach pales in significance to the damage caused to an institution's reputation.

And the instances of such breaches are alarmingly high: the ITRC estimates that at least 57 breaches – compromising the records of nearly 800,000 people – have been made at higher education institutions this year alone...

Read the full article at: www.universityworldnews.com/article.php?story=20101210220743524

In the News:

Updated rogue AV installs on Macs without password

By Elinor Mills, cnet
May 25, 2011

A new version of rogue antivirus malware that targets the Macintosh operating system does not need victims to type in their administrator passwords to install and infect the machine, a security company said today.

The latest version of the malware has been overhauled to look like a native Mac OS X application and is using the application name MacGuard, according to an Intego blog post. But particularly concerning is the fact that unlike previous versions, which were dubbed Mac Defender, MacProtector, and MacSecurity, MacGuard installs itself without prompting for the admin password.

"If Safari's 'Open safe files after downloading' option is checked, the package will open Apple's Installer, and the user will see a standard installation screen," the anti-malware company's post says. "If not, users may see the downloaded ZIP archive and double-click it out of curiosity, not remembering what they downloaded, then double-click the installation package. In either case, the Mac OS X Installer will launch."

"Since any user with an administrator's account--the default if there is just one user on a Mac--can install software in the Applications folder, a password is not needed," Intego says. "This package installs an application--the downloader--named avRunner, which then launches automatically. At the same time, the installation package deletes itself from the user's Mac, so no traces of the original Installer are left behind."

The MacGuard program is downloaded by the avRunner application from an IP address that is hidden using steganography in an image file in the Resources folder of avRunner, the post says.

Web pages that look like a Finder window and appear to be scanning the computer are bogus, Intego said. Users should leave the page, quit the browser, and quit the Installer application immediately if anything has downloaded, as well as delete any associated file from the Downloads folder. Also, users should uncheck the "Open safe files after downloading" option in Safari's General Preferences, Intego advises.

In an Apple support article yesterday, the company said "in the coming days, Apple will deliver a Mac OS X software update that will automatically find and remove Mac Defender malware and its known variants. The update will also help protect users by providing an explicit warning if they download this malware."

The malware keeps changing names and appearances. It is designed to trick people into paying for supposed anti-malware software that they don't need.

Related article:

Scareware takedown by FBI, international authorities results in two arrests

https://threatpost.com/en_us/blogs/scareware-takedown-fbi-international-authorities-results-two-arrests-062311

Read the full article at: news.cnet.com/8301-27080_3-20066174-245.html?tag=topStories2

CHAPTER 2 Recognizing and Responding to Security Issues

Sometimes, security issues aren't recognized right away, because it's difficult to tell the difference between your computer's everyday quirks and things caused by a security problem.

This section outlines a few common signs of possible security issues and what to do if they happen to you.

Possible Security Problems

Security problem: Computer compromise

The following are some potential signs that your computer may be infected with malware, such as a virus, worm, or other software that allows someone to control your computer remotely. Be aware, if this is the case, the only solution may be to reinstall all of your computer's software. For more information, see www.cit.cornell.edu/security/respond/wipeclean.cfm.

Learn to recognize potential signs that your computer has been compromised:

- Your antivirus software, anti-spyware software, or personal firewall reports a problem.
- When browsing the web, you see lots of popup windows, or your web browser takes you to different sites than expected.
- Your computer seems slower than usual, crashes more often, or runs out of disk space unexpectedly.
- You receive an email from Cornell Information Technologies alerting you that your network usage has increased significantly, even though you have not been using the Internet more than usual.
- While browsing the web, you are redirected to a Cornell IT Security "Spam Alert" page to stop you from visiting a compromised web site.

Security problem: NetID password theft

The following are signs that someone has possibly stolen your NetID password and may be using it, without your knowledge, to commit fraud or other crimes:

- You receive many notifications of undeliverable email messages, or notice changes to how your email is working.
- Your password stops working. This may indicate that whoever stole your NetID password has changed it.
- You notice changes to your personal information on university systems.

If you have any reason to suspect your NetID password has been stolen, you should change your password and your security questions immediately. For more about why NetID passwords are stolen, how it happens, how to spot it, and what to do if it happens, see Protecting Your Identity, page 13.

See In the News: Stolen passwords can make a real mess, page 12.

Security problem: Computer theft

Both laptop and desktop computers are subject to theft on and off campus. If a computer you use for Cornell work is stolen, immediately report it to your department's technical support staff. They will file a report with the Cornell Police. Do the same if you have lost any portable storage, such as external hard drives, USB thumb drives, CDs, DVDs, tapes, or diskettes.

If you don't have technical support staff, call to report the theft to the Cornell Police at 607 255-1111.

Never leave your computer alone in a public area. Any computer in a public area needs to be physically secured. See Away from Home and Work, page 62.

Responding to a Security Problem

If you suspect that your computer has been compromised, do the following:

1. If possible, disconnect the computer from the network. Do this by turning off Wi-Fi and unplugging your Ethernet cord.
2. Follow the guidelines below to contact someone for help.

Where to go first: Your department's technical support staff

You should always start with your department's technical support staff. They are in the best position to offer immediate help and guidance in determining if you have a security problem on your computer.

"I often get an email telling me backup has failed. Is this a security problem?"

Although this is not necessarily a sign of a security problem, it does have security implications, because your backup is what will be used to recover lost data should your computer be maliciously attacked, lost, or stolen.

Any time your computer behaves unusually, contact your department's technical support staff to report it. This way, even if the issue is not caused by a security risk, the problem can be addressed and you can work without unnecessary interruptions.

If you do not have technical support staff

If your department does not have technical support staff, or other arrangements for technical support, contact the CIT HelpDesk (phone 607 255-8990, visit 119 Computing and Communications Center, email helpdesk@cornell.edu). For current HelpDesk hours, see www.cit.cornell.edu/services/helpdesk/about.cfm.

If it is an emergency

For emergencies, call the Network Operations Center (NOC) at 607 255-9900. The NOC is staffed 24 hours a day, seven days a week.

About the IT Security Office

If there is a risk of data loss, your department's technical support staff will report security incidents to the IT Security Office, as required by Cornell policy. The IT Security Office will investigate known or suspect security problems.

If the IT Security Office detects a security problem on your computer before you are aware of it, both you and your department's technical support staff will receive an email notification. In addition, your network access may be restricted, and your web browser may redirect you to an online version of the notification.

Common security terms

Compromised computer – a computer that cannot be considered secure, because it has been stolen, infected with malware, accessed by someone without authority to access it, or subject to some other form of malicious attack.

Malware – a contraction of "malicious software," malware is a general term used to describe software that infiltrates or damages a computer.

Spyware – malware whose principal aim is to surreptitiously collect information by "spying" on the user.

Trojan – malware that appears to perform a benign or useful action, but actually performs a malicious action, such as transmitting a virus. A common Trojan is "free antivirus software" available on the web that is most likely a virus meant to spy on you!

Virus – self-replicating malware that attaches itself to a digital document or application, then spreads through shared copies of that document or application, frequently via email or USB drives. Viruses almost always corrupt or modify files.

Worm – self-replicating malware that can move from computer to computer on the network. Unlike a virus, it does not need to attach itself to an existing document or application. Worms almost always cause harm to the network, if only by consuming bandwidth.

In the News:

Stolen passwords can make a real mess

Excerpts from the article by Bill Steele, Cornell Chronicle
October 28, 2009

On Sept. 3 and 4, Cornellians found their messages to AOL and some other systems failing to arrive. Someone had sent about 330,000 spam messages using a Cornell email account, which caused several ISPs to block or slow down email from Cornell. AOL addresses were blocked until the following morning.

Then, at the end of September, large volumes of spam were sent from 17 Cornell email accounts, forcing CIT to change the passwords for those NetIDs.

...In this case the problem was not hacked computers but stolen NetID and password combinations. "Compromised NetIDs are a bigger spam problem than compromised computers," said Tom Young, interim director of CIT's IT Security Office.

Spammers can use your NetID and password to send mail, either by connecting directly to a Cornell email server or using Webmail, so they are able to hijack Cornell servers to do their dirty work. Malicious individuals can also use stolen NetIDs and passwords to log into or disrupt other services, including some that hold sensitive information.

NetIDs and passwords are commonly stolen through "phishing" email scams. An official-looking email says your email account is over quota or needs to be re-registered by clicking on a link in the message. The message is in HTML format, which means that what you see on the screen is not the actual text. A link that looks like http://citmail.cornell.edu may actually go to http://someplace.else.co.za. (The .za in this example means the site is in South Africa, probably on a compromised computer; the scammers may actually be in St. Louis.) The link takes you to what looks like a real Cornell web page where you are asked to log in with your NetID and password.

The 17 people whose accounts were appropriated at the end of September were fooled by a perfect replica of the standard Cornell CUWebLogin dialog.

A disproportionate number of people who fall for phishing scams are located off campus, including Cornell Cooperative Extension agents, retirees and emeritus faculty. These people are often more susceptible because they don't have someone they can easily turn to and ask whether an email message purporting to be from Cornell is legitimate, so they play it safe and answer the message. "These schemes play on people's fears," noted Young.

Many phishing messages contain misspelled words or look like they were written by someone just learning English, but some scammers are more sophisticated. One message announced quite convincingly that users needed to "validate" their accounts to help combat spam.

"CIT is looking into better approaches to blocking phishes and to protecting our email system from the impact of a stolen NetID," said Young.

Meanwhile, CIT faces a Catch-22. They can stop the spam by changing the password for the stolen account, but then they can't notify the user by email.

"We hate the inconvenience we cause when we change someone's password," Young explained, "but we're caught between a rock and hard place. We have to protect the integrity of university operations, even if it means disrupting an individual's ability to access the campus services that require a NetID."

Read the full article at: www.news.cornell.edu/stories/Oct09/netIDcomp.html

CHAPTER 3 Protecting Your Identity

Identity theft is a rapidly growing threat, and it thrives on poor security practices. Your best defense is to build good security habits and encourage everyone you know to do the same. For ***22 steps to protect yourself from identity theft – and 8 ways to clean up things if you become a victim***, see Your 5-minute guide to protecting your identity by MSN Money (articles.moneycentral.msn.com/Banking/FinancialPrivacy/TheFiveMinuteGuideToProtectingYourIdentity.aspx).

If you believe you may be the victim of identity theft, contact your local community law enforcement or the Cornell Police at 607 255-1111 to file a report.

> *"Identity theft is a serious crime. It occurs when your personal information (name, Social Security number, date of birth, credit card number, or bank account number) is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your good name."*
>
> *Federal Trade Commission, www.ftc.gov*

NetID Password Theft

At universities across the country, the theft of electronic IDs assigned to faculty, staff, and students, such as Cornell's NetIDs, is a rapidly growing problem.

Your NetID is your online identity at Cornell. Used with your NetID password, it provides access to your personal information and is the key to using a variety of campus services, such as email.

For many of us, it also provides access to other people's data. Protecting data placed in Cornell's care by faculty, staff, and students is part of being a responsible network citizen. **Keeping your NetID password safe is one way you can help protect everyone's data on campus.**

If someone steals your NetID password, they can gain access to any service that you can access with your NetID:

- Spam can be sent using your Cornell email. If this happens both you and the university could suffer consequences:
    1. The university email system could get blocked by Internet service providers who identify spam being sent from Cornell mail servers – spam from your email could potentially get everyone at Cornell blocked.
    2. You could lose time and productivity if the IT Security office needs to scramble your password, or if you receive a large number of bounced messages and complaints.
- Technical journals and other licensed Cornell Library resources can be accessed, putting Cornell at risk of being blocked from using the resources or having the university license revoked.
- Your personal university information can be accessed, putting you at risk for identity theft.
- Depending on your job function at the university, sensitive or confidential information about other members of the community could be exposed to unauthorized individuals.

How NetID passwords are stolen

You are tricked into giving away your NetID password

These days we are overwhelmed by fraudulent email messages and web sites that try to steal personal information. These are often referred to as "phishes." A common trick is to suggest that one of your accounts will be shut down unless you reply immediately with your password and other information.

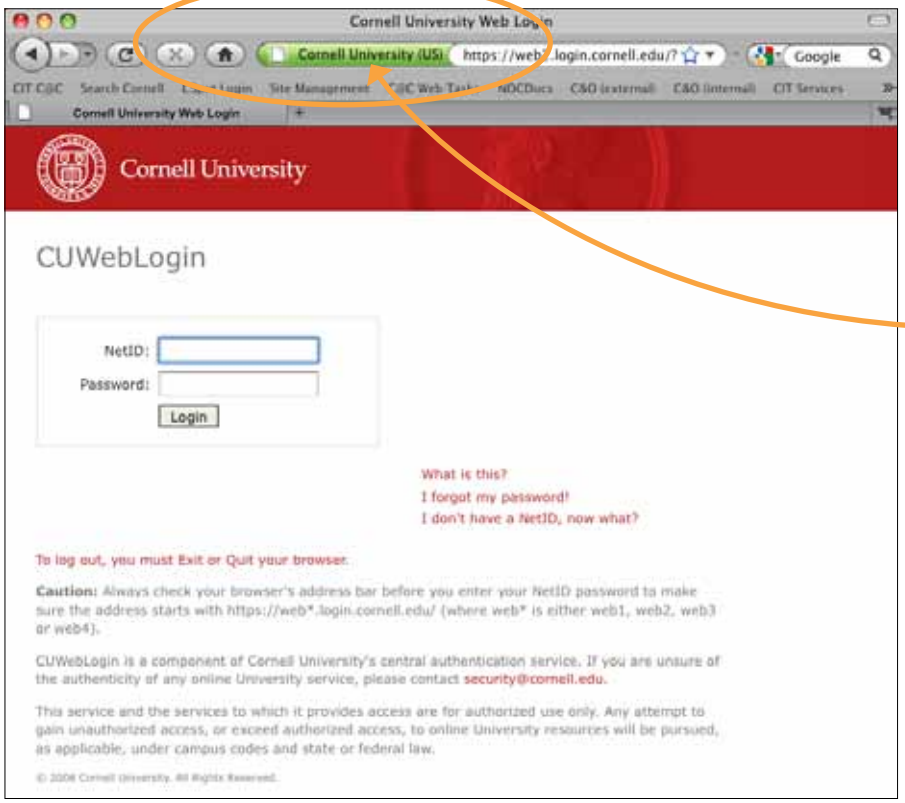
No one should ever ask you for your NetID password – not in email, not on the phone, not in person.

Sharing your NetID password is a violation of university policy

Never share your NetID password with someone else. No one besides you should know your NetID password. Not your supervisor, not your assistant, not your technical support staff, not your family members, spouse, or friends.

You type your password into a fake Cornell web site

Watch out for CUWebLogin and Outlook Web Access knockoffs! Malicious web sites may include a plausible-looking or even an exact copy of either of these pages.



Make sure you are really signing in at the Cornell CUWebLogin page.

See Look for Extended Validation Certificates (EV Certs), page 46.

You use your NetID password for a non-Cornell account

Using your NetID password for other services, such as online banking, shopping, or discussion forums, increases the chances that it may be stolen, because these services may not transmit the password securely or could experience a security breach.

In December of 2010, gawker.com had around 1.3 million passwords (including corresponding usernames and email accounts) compromised, several of which belonged to people at Cornell. As is often the unfortunate case, some people were using their NetID as their username, or their Cornell email (which includes their NetID) for the non-Cornell web site.

The data was a "dream come true for spammers," reported news.softpedia.com (see In the News: Hackers compromise Gawker, expose user passwords, page 23). Since experience demonstrates that people often use the same password for most online accounts, hackers immediately began attempts to access Cornell email accounts using the exposed Gawker password and NetID information.

Avoid using your NetID as your login or account name for any non-Cornell services. If you have no choice, because the web site automatically uses your email address for the account name, make sure to choose a password that has no similarity to your NetID password.

Your NetID password is too simple

Contemporary computers are so powerful that simple passwords can be cracked with minimal effort. See How to Create a Strong NetID Password, page 19, to find out what makes a strong password. To test your password's strength, go to the Manage Your NetID page at netid.cornell.edu and click **Do you have a strong password?**

Your computer is infected with software that snoops for your NetID password

Sometimes a computer infection includes a keylogger, software that records everything you type and then sends it off to whomever has taken control of your computer. The intruder can then see your password as it's typed. This is less common, but needs to be considered if no other explanation is found.

You type your password on a computer open for public use

Entering your NetID password on any unfamiliar computer puts you at risk. What assurance do you have that it is protected by good security practices? Public computers, such as are found in hotel lobbies or cafes, are particularly dangerous because it's possible someone unscrupulous has installed malicious software to steal your personal information. If you must enter your NetID password on a computer that's meant for public use, change it the next time you are on a trusted computer.

Common Campus Services that Require Your Password

Some campus services, including the following, don't use CUWebLogin, although they still require your NetID password to sign in and they are also secure:

- Cornell's Exchange email and calendar service, accessed via Outlook, Entourage, Outlook Web Access, MyCornell, or another client
- MyCornell – The campus web portal
- COLTS – Online timecards
- Employee Essentials, Who I Am, and other services for managing your personal university information
- Eduroam or RedRover-Secure – Cornell's secure Wi-Fi services
- Cornell VPN – The campus Virtual Private Network service
- Faculty Center – Tools faculty use to advise students and maintain class information

- Blackboard – Course information and materials
- Confluence – Collaborative project site
- Other web-based applications that use CUWebLogin

When in doubt, before you enter your NetID password, check with your technical support person or the HelpDesk (phone 607 255-8990, visit 119 Computing and Communications Center, email helpdesk@cornell.edu).

How to spot NetID password theft

If your NetID password is stolen and your NetID is used to send email spam, there can be a number of warning signs:

- You start receiving large numbers of messages that were rejected by spam detection systems or returned due to bad addresses.
- You get complaints from people who think you sent them spam messages. (Note that this can also be the result of someone forging your email address, but not using your email account.)
- You find messages in your sent folder that you know you didn't send. The spammer using your email account may not clear out copies of the messages that were sent.
- You are missing email that you saved or that you know was sent to you. Sometimes the person using your email account will delete all your stored messages so you don't find copies of the spam emails that were sent out, or the rejection and complaint emails sent to you.
- You see unexplained changes to your Outlook Web Access (OWA) or Who I Am settings. The spammers may change the name that appears in messages sent from your account, the signature you add to the bottom of messages, or even how your email is routed.

Your email isn't the only indication. Here are some other signs your NetID password may have been stolen:

- Your password stops working. Someone may have changed it, to stop you from resetting it yourself.
- You note unexpected changes to your personal university information (address, phone number, benefits, schedule, etc.).
- You suspect that one of your non-Cornell online accounts (at a bank, store, blog, etc.) may have been compromised. Any compromise could potentially put your NetID password at risk, especially if you use your NetID password for that service (a bad practice).

What to do if you suspect your NetID has been stolen

1. Change your NetID password and your security questions immediately.

To change your password, go to the Manage Your NetID page at netid.cornell.edu and click **Change your Password**. Your new NetID password should be unique and strong:

- It should not be similar to the old password.
- It should not be the same as or similar to any passwords you use for other purposes, such as online banking or shopping.
- It should be easy for you to remember and difficult for other people to guess. See How to Create a Strong NetID Password, page 19.

To change your security questions, go to netid.cornell.edu and click **Set your Security Questions**. If you have not previously set your security questions, do so now. Setting your security questions will allow you to set a new password without visiting the CIT HelpDesk, should you ever forget your current password.

Have you set your security questions?

Don't wait until you have a password problem! If you haven't already done so, set your NetID password security questions now.

Doing so will allow you to reset your password without visiting the CIT HelpDesk, should you ever have an issue.

Go to netid.cornell.edu and click **Set your Security Questions**.

If you cannot change your password!

Sometimes whoever is using your stolen NetID will change your NetID password. In addition, if the IT Security Office determines that your password has been compromised, they may scramble your password, before contacting you, to stop further abuse. If either happens, you will need to contact the CIT HelpDesk to reset your password (phone 607 255-8990, visit 119 Computing and Communications Center, email helpdesk@cornell.edu).

- To set a new password at the CIT HelpDesk, you must appear in person and present your Cornell ID card or a government-issued photo ID card.
- If you are not currently in Ithaca, you must fax or mail a copy of a government-issued ID card to the HelpDesk. Instructions for setting a new password will be sent to you by U.S. mail.

2. Check your Cornell personal information.

If your NetID email account was used to send spam, you should check Outlook Web Access (OWA) and Who I Am to make sure your email settings have not been changed. For instructions on how to check your Cornell personal information, see www.cit.cornell.edu/security/identity/netidtheft/whattodo.cfm#check.

3. Report the incident immediately.

Don't hesitate. Any possible or confirmed theft of a NetID password needs to be reported immediately to the IT Security Office via security@cornell.edu. You should also notify your department's technical support staff.

The IT Security Office may contact you for additional information since, to help prevent this in the future, they try to determine how a password was stolen. Computer records can also be looked at to see what services your NetID accessed, and how long it was abused.

How to Create a Strong NetID Password

Make all of your passwords, but especially your NetID password, as long and complex as feasible. Your passwords should be easy for you to remember, and difficult for other people to guess.

Cornell's password complexity rules may seem challenging at first. When you see examples like this – H*P@p7mZ% – you might wonder how anyone ever remembers their Cornell password.

The secret is finding the password recipe that works best for you. Use the rules below and find out if your password is strong enough by using CIT's Check Your Password resource at netid.cornell.edu/psc/lookup.html.

Password complexity rules

Your password should be at least 8 characters, including at least three of these four character types:

- Uppercase letters
- Lowercase letters
- Numbers
- Symbols found on your keyboard, such as blank spaces, or ! * - () : | / ?

Never use the following:

- Your NetID
- Your first or last name
- Dictionary words with 5 or more letters, including names such as "Cornell"
- Repeated characters (AAA or 555)
- Common sequences (abc, CBA, 123, 321, qwerty, pas)

"I share my password when I go on vacation, so my teammates can check my email."

Sharing your NetID password is a violation of university policy. Remember that your email is not the only thing that your NetID password protects.

It also protects information about your salary and benefits, as well as access to many university resources. If you have a need to share emails with others, consult your department's technical support staff for alternatives, such as an Exchange Group Account.

Recipe for your NetID password

1. Choose your main ingredient plus a number.

Examples of main ingredients

- A line from a favorite song, poem, or book
- The punch line of a joke
- A sports chant
- A personal memory that is unlikely to be public knowledge. "Firsts" can be a good choice, such as your 1st date, your 1st job, your 1st teacher, your 1st roommate, or your 1st car.
- A series from your life, such as the streets you've lived on; pets from your childhood; the names of your cousins; companies you've worked for; places you've visited or places where your family or friends live.

Examples of numbers

- Year, or month and year (but not your birthday)
- Quantity
- Price
- Age
- Part of an old phone number
- A personal best from a sport (score, distance, time)

Do not use any of the example passwords shown here.

2. Combine your main ingredient and your number to create your Cornell password.

Method 1: Chop (Passphrases)

Create a phrase or sentence. Add a comma, colon, semi-colon, period, or exclamation point if your phrase didn't come with punctuation. Then abbreviate most of the words. (Your passphrase can have words shorter than 5 letters, as long as those words are less than 40% of the total.) For example:

- Parts of people's names + number + symbol:

  "Barbara and John" with the meaningful year 2010 becomes 2010Bar+Jo

- A phrase, with longer words abbreviated, + symbol + number:

  "Libe Slope legs" with a 15% slope, becomes Libe Slpe legs=15%

Method 2: Shred (Acronyms)

Create a phrase or sentence. Add a comma, colon, semi-colon, period, or exclamation point if your phrase didn't come with punctuation. Then take the first letter of each word. For example:

- "This grand institution, this school of Cornell!" plus a 10th reunion in June 1992 becomes 10thTgi,tsoC!0692

Method 3: Puree (Secret Codes)

Invent a secret code that you use for any passwords you create, not just your Cornell password. Apply your secret code to passphrases, acronyms, or words. For example:

- Capitalize the first letter of every word.
- Change certain letters into symbols or numbers (but be creative and avoid these overused and too-obvious substitutions: the number 0 for the letter o, the symbol @ for the letter a, the number 1 for the letter l, and the number 3 for the letter e).
- Decide what to do with spaces: Don't use any, keep some, or replace some with a specific symbol or number.
- Put your meaningful number in a specific spot.

Example of a secret code password:

- "Stone, Roberts, East Roberts" plus the first month at Cornell, August 1975, becomes St%08, R%b, E^s75R%b

The rules for this secret code: The first letter of every word is capitalized. Each word is abbreviated to the first three letters. The letter a is the symbol ^ and the letter o is the symbol %. The spaces that follow the commas are kept. The first part of the number goes after the first word, and the last part of the number goes before the last word.

For steps to creating a strong password, see You're Smart; Your Password Should Be Too at www.cit.cornell.edu/security/identity/passwords/strong.cfm.

Best Practices for Managing Passwords Safely

Most users today have to keep track of sometimes dozens of passwords: for Cornell resources, online banking, e-commerce sites such as eBay or Amazon, and other web sites.

University policy forbids using your NetID password for other sites, and it is a poor security practice to use the same password for all sites, so multiple passwords are a requirement.

Create unique, strong passwords

- One for your Cornell NetID
- One each for any services that you want to keep very secure, such as logging on to your computer, online banking, or other key personal matters
- One in common for services where you are less concerned about security or if other people access the information

Consider using a password storage utility

The most secure way to store and manage passwords is to use one of many available password storage utilities. These utilities allow you to create one **very strong password** that is then used to encrypt and store all other passwords. For a list of recommended password storage utilities, see www.cit.cornell.edu/security/identity/pwdstorageutils.cfm.

Use caution if writing your passwords down

Obviously, the more passwords you have to use, the greater the temptation to write those passwords down to ensure they are remembered. If you need to write down a password, make sure the account with which it is associated is unclear. For example, do not write down the URL for your bank with your password written next to it. Instead, either write down the password, without listing what the password belongs to, or pick a word or phrase that will remind you of your bank, without being obvious.

For example: If you had a money bank shaped like a cat when you were a kid, you might write "cat" next to your bank password to help you remember that it is your bank password.

Keep people from trespassing on your computer

Make sure the password that unlocks your computer is not used for any other purpose, and that it is strong.

Don't use "remember password" utilities in your web browser or email client. They make it easy for someone to log into your accounts if they gain access to your computer.

Encrypt any passwords stored on your computer. It does not matter how complex your passwords are, if someone can find them. Your passwords should always be kept private.

Why do I have to choose a complex password for my NetID?

Your NetID and password control access to highly confidential data, some of which requires protection mandated by federal legislation. Tools for cracking simple passwords are readily available, so it is essential that your NetID password be strong to prevent unauthorized individuals from discovering it.

Complex passwords are akin to deadbolt locks on a door. Just as deadbolt locks are far more effective than standard locks in preventing break-ins, so are complex passwords far superior to simple passwords in protecting access to your information.

In 2002, the university auditor recommended that CIT implement technical measures to ensure that users choose secure NetID passwords. The criteria for what constitutes a secure password were developed as a result, along with the web-based method for selecting a password.

In the News:

Hackers compromise Gawker, expose user passwords

By Lucian Constantin, Softpedia
December 13, 2010

Gawker Media is dealing with a serious security breach after hackers managed to compromise several of its servers and leaked a database of 1.3 million usernames and passwords.

In a network-wide announcement, Gawker warns users who have an account on any of its ten highly-trafficked blogs, which include Gizmodo, LifeHacker, Jezebel and Kotaku, that their passwords were compromised.

"We understand how important trust is on the internet, and we're deeply sorry for and embarrassed about this breach of security—and of trust," the media company says.

"We're working around the clock to ensure our security (and our commenters' account security) moving forward," it adds.

A group called Gnosis took credit for the attack and it seems that its motive was Gawker's taunting of Anonymous and 4chan members, which at one point it called "script kiddies."

"Previous attacks against the target were mocked, so we came along and raised the bar a little," Gnosis said. "You wanted attention, well guess what, You've got it now!" it added.

Gnosis notes that the hacked database contained the login details of 1.5 million users, of which 1.3 million were copied and leaked online.

The problem is the data didn't contain only usernames and passwords, but also email addresses, making it a dream come true for spammers.

In addition, the algorithm used to encrypt the passwords is weak and can be cracked rather easily. In fact, hackers have already done this for a number of accounts including those of Gawker editors.

Previous incidents of this type have shown that a lot of people use the same password for all or most of their online accounts. It's therefore fair to assume that decrypting the Gawker passwords will give hackers access to many of the listed email accounts.

"You should immediately change the password on your account, and if you used that password on any other web site, you should change your passwords on all of those accounts as well," Gawker advises in a FAQ about the incident.

It also seems that the compromise was much more extensive than the user database and involved Gnosis obtaining access to other Gawker data as well, such as 4 GB of internal chat logs, FTP passwords and confidential emails.

Read the full article at: news.softpedia.com/news/Hackers-Compromise-Gawker-Servers-Expose-User-Passwords-172180.shtml

CHAPTER 4 Protecting University Data

You are responsible for Cornell data stored on computers you use. You are the custodian of that data. This is established in numerous Cornell policies. See Appendix II: An Overview of University Policies on Computer Security and Data Protection, page 68.

Your responsibilities:

- Protect university property stored on computers you use, including information about staff, faculty, students, and alumni.
- Access only that information which you are authorized to access in the course of your duties. Your ability to access other information does not imply any right to view, change, or share information.
- Do not establish access privileges for yourself or others outside of formal approval processes.
- Adhere to procedures and business rules governing access and changes to the data for which you are a custodian.

As stated in University Policy 4.12, Data Stewardship and Custodianship, the university expects all stewards and custodians of its administrative data to manage, access, and utilize this data in a manner that is consistent with the university's need for security and confidentiality. Cornell University administrative functional areas must develop and maintain clear and consistent procedures for access to university administrative data, as appropriate. See www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/governance/data.cfm.

See In the News: Data security breaches often triggered by carelessness, page 32.

Know What Information Is on Your Computer and Secure It

Be aware of what types of information are stored on your computer and take steps to protect it. Cornell Policy 5.10, Information Security, establishes three data security classifications:

- Confidential – Specific data elements subject to more stringent security requirements.
- Restricted – Unless otherwise classified, all information used in the conduct of university business is restricted, and not open to the general public.
- Public – University data that has been explicitly made available to the public, with no authentication required for network access.

All information at Cornell should be protected. Even data that you may not consider sensitive should be protected. Take appropriate measures, outlined in this security handbook, to protect university data, wherever you are and whatever computer you are using.

Examples of the diverse types of data seen at Cornell

Cornell is like a small city. People work, study, live, and play here. We have our own transportation, dining, administration, residence halls, and offices. As a result, there is a wide variety of university data, which you may access or use for your work or in your day-to-day life at Cornell. Some examples include:

- Employment records
- Background checks for employees
- Budget information
- Cornell ID card numbers and info that's associated with parking, buying food, or bus access
- Credit card, departmental account, or procurement card numbers
- Email
- Emergency planning information
- Financial aid data
- Financial records
- Grades
- Grant information
- Health insurance
- Human resources records
- Infrastructure data: building plans, control systems, utilities, networks, etc.
- Investment information
- Letters of recommendation
- Library circulation records
- Loan records
- Name, home address, phone
- Non-public directory biographical data
- Payroll
- Research data
- Salary data
- Tax records of the university, its employees, parents, and students
- Travel arrangements
- Vehicle registration
- Video surveillance
- Voice mail

University Data Currently Classified as Confidential

In addition to being subject to Cornell policies and processes, confidential data is subject to more stringent security requirements, as outlined in this chapter and in Securing Your Computer, page 34.

Data currently classified as confidential includes the following, when they appear in conjunction with an individual's name or other identifier:

- Social Security numbers
- Driver's license numbers
- Credit card numbers
- Bank account numbers
- Protected health information

This set may expand based on future regulatory requirements or designations made by the appropriate university data steward. Data stewards are senior officers of the university responsible for determining how data in their area should be handled. For example, the Vice President for Human Resources is the data steward for administrative data pertaining to Cornell employees. The data steward role is defined in University Policy 4.12, Data Stewardship and Custodianship (www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/governance/data.cfm).

State and federal legislation

In addition to the other measures outlined in this handbook, some data at Cornell is subject to the following:

State Security Breach Notification laws

- Social Security numbers
- Credit card data
- Driver's license numbers
- Bank account information

Health Insurance Portability and Accountability Act (HIPAA)

- Health insurance
- Health records/patient treatment information

Gramm-Leach-Bliley Act for Disclosure of Nonpublic Personal Information (GLBA)

- Loan records

Family Educational Rights and Privacy Act (FERPA)

- Tax records of parents and students
- Grades

Sarbanes-Oxley Act

- Cornell tax records

Handling Sensitive Data

General considerations

These general concerns are beneficial to everyone, but they are particularly important if you work with confidential data or other sensitive information.

1. Keep what you view on your computer screen private. Consider if it is possible for someone to walk into your workspace and see sensitive data on your screen. Take steps to prevent this, such as turning your monitor or using a privacy screen.

2. Keep your equipment safe. One of the most common ways data is lost is via stolen hardware. Don't give someone an opportunity to walk off with equipment where you keep sensitive data, such as your computer or portable storage devices. Sensitive data stored on devices you take out of your workspace is at particular risk. Steps to prevent hardware theft include locking your computer with a security cable and storing small devices out of view when they aren't in use, preferably in a locked drawer or cabinet.

3. Keep security in mind whenever you work off campus. Review Working Off Campus, page 60, to learn why you should use the campus Virtual Private Network, the importance of setting up a secure home wireless network, and why you should be extra careful when using public computers.

4. Back up your data regularly. Find out what backup solution your department recommends to keep data backed up. Regular backups provide the following security benefits:

    - Protection against losing all of your work.
    - Help determining what sensitive data may be at risk if your computer is lost or stolen.

Do-it-yourself backup solutions pose risks!

With do-it-yourself backup solutions, data may be backed up on an irregular basis, or it may put confidential data at risk by storing it on an external hard drive that is easy to steal.

For this reason, do-it-yourself backup solutions are discouraged. Use a backup service that guarantees data is backed up regularly and stored securely. Contact your department's technical support staff for recommendations.

Handling paper documents with confidential data

When you work with printed material containing confidential data, handle it responsibly:

- Secure documents, so they are only accessible to authorized personnel (lock them in a drawer, cabinet, or office).
- Never leave documents unattended in a public area.
- Destroy or securely archive documents no longer needed for daily operations.
- Require a signed receipt of delivery when you send documents off campus.
- Seal and stamp "Confidential" all documents sent through campus mail.
- Destroy documents using a secure disposal service or a cross-cut shredder.
- If you fax or print a document, make sure the receiving device is in a secure location.

For full details, see Policy 5.10, Information Security, Security of Paper Documents (www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/informationtech/infosecurity.cfm).

Specific requirements for confidential data

1. Encrypt any passwords stored on your computer that access confidential data.
2. Keep confidential data stored only as long as is necessary to complete the work for which it is intended, regardless of whether the confidential data is stored on your computer or a departmental file server.
3. Always transmit confidential data securely:
   - a. Do not send confidential data in an email, in the body of a message, or in an attachment, unless the data is encrypted. The Windows version of Microsoft Office 2007, and later versions, includes a utility for appropriately strong encryption of documents. The password-protection feature found in Office for the Mac and older versions of Word and Excel for Windows is not sufficient to fulfill the requirement of encrypting confidential data.
   - b. Do not send confidential data in an instant message (IM) or a text message.
   - c. If you have not been instructed by your technical support staff to use some other approach, use Cornell Dropbox to exchange sensitive data with others at Cornell. See dropbox.cornell.edu.

4 Do not store confidential data on a file server unless it is in a folder that can only be accessed by people authorized to see it.

5 Do not store confidential data on a server that is also used to host a public web site.

6 Encyrpt any confidential data stored on a laptop, notebook, or other mobile device.

See Additional Requirements for Computers and Mobile Devices Storing Confidential Data, page 37.

Consequences of Mishandling Sensitive Data

Mishandling sensitive data can lead to Cornell suffering financial loss or damage to its reputation. The law requires Cornell to report the possible loss of certain types of data to government agencies and notify potentially affected individuals.

If there is any possibility of data loss, responding can easily consume hundreds of hours and is, as a result, an expensive activity. It can also involve many people from both within your department and elsewhere around campus and, consequently, can significantly disrupt university business.

Losing sensitive data has repercussions:

- Regulatory fines
- Loss of funding from government agencies
- Lawsuits
- Loss of donations and gifts
- Loss of reputation

See, In the News: Most companies not erasing sensitive data, page 33.

What Happens When Cornell Data May Have Been Exposed to an Intruder or Malicious Software

If an intruder has gained access to a computer used at Cornell that contains sensitive data, the IT Security Office will lead an investigation of the incident:

1 The computer's hard drive is copied for analysis.

2 Information on the computer's hard drive and other data, such as network traffic history, are analyzed to determine whether sensitive data may have been exposed.

What should I do with my old computer when it's time to throw it out?

When you retire hardware, be it your old computer, thumb drive, or a stack of CDs, it is necessary to take steps to sanitize and dispose of data appropriately, so it cannot fall into malicious hands. If your computer or other media stores confidential data, give it to your department's technical support staff for proper disposal.

See Best Practices for Media Destruction to learn about IT Security Office recommendations (www.cit.cornell.edu/security/depth/practices/media_destruct.cfm).

3 The university's response to the incident is determined by the Data Incident Response Team (DIRT) members:

- Vice President for Information Technologies (chairs the group)
- IT Policy Office
- IT Security Office
- Audit Office
- University Counsel
- Cornell Police
- University Communications
- Risk Management

4 The DIRT team also brings in the unit head, technical support staff, and other staff from the department where the incident occurred, as well as the university data steward (for example, the Vice President for Student and Academic Services for incidents involving student data, or the Vice President for Human Resources for incidents involving employee data). For a complete list of data stewards, see University Policy 4.12, Data Stewardship and Custodianship (www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/governance/data.cfm).

5 DIRT meets to review the incident and determine how the university should respond to it. If there is a reasonable likelihood that sensitive data could have been accessed in an unauthorized fashion, DIRT determines which potentially affected parties need to be notified. DIRT also considers what needs to be done to avoid similar incidents in the future.

Why Data Security Is Important

In departments that have not yet implemented a formal data cleanup process, some two-thirds of staff computers are storing other people's confidential information.

With identity theft due to the loss of online data a major concern these days, Cornell needs to better protect sensitive data stored in electronic form, particularly the personal information that students, employees and others associated with Cornell have placed under the university's trust.

- **Regulations protect certain types of data.** See, University Data Currently Classified as Confidential, page 26.
- **A security breach has financial and reputation repercussions.** The university has the direct expense of generating the notifications and providing credit-monitoring services. The worst cost, however, is the damage a data breach does to Cornell's reputation—with the campus community, with our supporters, and with the general public.

You are the solution

Sensitive data is spread far and wide throughout campus, including on staff laptops and desktops and on local file servers. Accepting individual responsibility for the university information entrusted to your care is essential.

Finding where confidential data is stored, removing what is no longer needed, and appropriately securing what must be retained are the best steps you can take to improve data security.

Data Discovery Software

Data discovery software is used to search a computer for sensitive information, including some of the types of data Cornell has classified as confidential, such as Social Security numbers and credit card numbers.

A data discovery software program examines the documents on a computer's hard drive, or a specified portion of the hard drive, looking for possible instances of sensitive information. Removable or external drives and network shares can also be scanned.

Depending on how much material is on the disk, and how powerful the computer is, this scanning process can take a significant amount of time. Once the scan is complete, you can review the results.

For each instance of what might be sensitive data, the data discovery software shows you where it was found and gives you the choice of:

- Securely deleting (shredding) the file in which it appeared, or editing out (redacting) the sensitive data;
- Setting the file aside in a special location; or
- Taking no action.

Follow your department's local practices!

Contact your department's technical support staff to inquire about local practices around data discovery.

For more information about searching your computer for sensitive data that the university has classified as confidential, see the Guide to Data Discovery at Cornell (www.cit.cornell.edu/services/guides/data_discovery/index.cfm).

Old information is risky information!

As often as not, sensitive data putting Cornell at risk is no longer relevant to current work and the person using the computer is not even aware of it. The most common problem is files dating back to when Social Security numbers were still being used as a general identifier. Sometimes these are files from a previous user of the computer.

In the News:

Data security breaches often triggered by carelessness

Excerpts from the article by Pamela Lewis Dolan, American Medical News
February 22, 2010

Often the biggest threat to your practice and patient data is not an outside hacker or a snooping employee -- it's somebody's forgetfulness.

As technology becomes smaller and more portable, it becomes easier to lose. Surveys from a data protection solutions company in 2009 found that in a six-month period, 12,500 mobile devices were left in taxis, and 4,500 USB memory sticks were left in pockets of pants sent to dry cleaners.

Most people -- including those in the security business -- are not protecting the data on their mobile devices. So if the device is lost, the data could be accessed.

"I'm always surprised at the cowboy attitude," said Harry Rhodes, director of practice leadership for the American Health Information Management Assn. "You've got these people who think, 'What are the odds of that happening to me?' And then when it's happening to you, it's too late to do anything."

Just having your phone drop out of your pocket could launch a time-consuming and expensive nightmare of reconstructing data and adhering to fixes mandated under the Health Insurance Portability and Accountability Act.

Provisions in the federal stimulus package have tightened HIPAA notification and enforcement regulations and have made HIPAA violations more costly. For example, the maximum civil penalty from the Dept. of Health and Human Services for a data breach occurring after Feb. 18, 2009, rose from $25,000 to $1.5 million.

So how you do protect yourself from an accidental loss of a device containing sensitive data? Experts recommend two strategies. One is to find a way to handle or store your mobile technology so you can't lose it easily. The other is to make sure the device has security and encryption features that make it next to impossible to access by anyone who happens to find it.

...Credant Technologies, a Dallas-based data protection solutions company, noted in a 2008 survey that although more than a third of health care professionals store patient data on laptops, smartphones and USB memory sticks, most do not adequately secure the data.

... Rhodes has seen organizations block USB ports on desktop computers with a plug-in device or a super glue product, preventing data from being exported onto a thumb or flash drive.

He said there also are software packages that can be downloaded onto PDAs or smartphones that allow the users, in the event the device is lost or stolen, to call a phone number that automatically will erase everything from the device. There also are downloadable GPS systems that can help locate a lost device.

Smartphone and thumb-drive users also should use password protection on the devices, experts said. Use of a password to enter the system is just an additional line of defense that should be coupled with encryption -- the most effective means of protection available, they said...

Read the full article at: www.ama-assn.org/amednews/2010/02/22/bil20222.htm

In the News:

Most companies not erasing sensitive data

Excerpts from the article by Melissa Klein Aguilar, Compliance Week
November 16, 2010

Most businesses don't properly erase sensitive data from old computers and hard drives, leaving them highly susceptible to data breaches, according to a survey by Kroll Ontrack.

Only 49 percent of more than 1,500 respondents polled worldwide say their businesses are systematically deploying a data eraser method. Among that group, 75 percent don't delete data securely, according to Kroll.

Maybe they didn't hear about the digital copier incident that resulted in one company notifying more than 400,000 people that their personal or medical data may have been compromised. As Compliance Week previously reported, in April, Affinity Health Plan had to send a breach notice to more than 400,000 of its customers after CBS News, as part of an investigation, purchased a digital copier previously owned by Affinity from a wholesale warehouse and discovered that the copier's memory contained individual medical records and non-medical documents including driver's licenses and Social Security cards.

... In addition to helping companies comply with data privacy and retention laws and regulations, data wiping is fundamental to reducing the risk of security breaches.

"It is a must - regardless of the size of the organization - and needs to be incorporated into overall data security and business continuity plans," he says.

Certified data wiping software that overwrites all the data on the hard drive or a degausser, which wipes the data using a strong magnetic force rendering the device no longer usable, are the two safest methods to ensure private data is wiped, according to Reinert.

Only 19 percent of those responding say their company deploys data eraser software and just 6 percent use a degausser to erase media. Roughly a third of businesses "do not know" how they ensure their data has been erased from an old device, while 22 percent say they "reboot the drive" to see if the data is still there.

In total, Kroll notes that more than 60 percent of all old business computers are fully intact with proprietary business data in the second-hand market. Forty percent of those polled say their companies gave away their used hard drive to another individual, and 22 percent don't know what happened to their old computer.

Cornell has procedures around data destruction

See www.cit.cornell.edu/security/depth/practices/media_destruct.cfm

Read the full article at: www.complianceweek.com/most-companies-not-erasing-sensitive-data/article/191903/

CHAPTER 5 Securing Your Computer

> "It would be convenient if we could solve security problems by installing a piece of technology, but the truth is that security is as much an issue of people and process as it is technology."
>
> Diana Oblinger and Brian Hawkins, EDUCAUSE
> educause.edu

If your computer is insecure, you are putting not only your own work at risk but also that of others at Cornell.

Following the steps outlined here will greatly improve the overall security of your computer. All of these measures are mandated by the university's baseline IT security requirements, and apply to all campus systems used to conduct university business.

If your department has technical support staff, consult with them about preferred practices.

Secure all operating systems on your computer!

If you have a Mac that runs Windows, make sure you secure both.

Set a Strong Password for Access to the Computer

Your computer must be configured so that when it starts up, you need to enter a password.

- If you are not using CornellAD, this should be a strong password that is only used by you. It must not be the same password as your NetID password.
- If your unit has started using CornellAD, you will use your NetID and NetID password to log in.

These requirements apply to all accounts on the computer. Any access to your system must be protected by a strong password. As a guide to creating strong passwords in general, see How to Create a Strong NetID Password, page 19. It's possible, however, that your department's technical support staff may enforce different (even more stringent) rules for setting your computer's login password.

Keep Your Software Updated

Without up-to-date software, the average unprotected computer connected to the Internet can be compromised in less than a minute. This means the single most important step to securing your computer is making sure you always have all the current updates to key software packages installed. This includes your operating system, web browser, email program, all other applications that connect to the network, and Microsoft Office.

You can configure your computer to automatically run Windows Update or the Mac OS Software Update daily. To learn how, see www.cit.cornell.edu/security/howto/browserupdate.cfm.

Run Up-to-Date Antivirus Software

Always run antivirus software configured for daily updates and active monitoring.

Antivirus software will help keep your computer free of malicious software such as viruses, worms, and trojan horses. You also need to protect yourself against spyware and adware, which could gather your personal information or create an opening for more serious threats. (For definitions of common security terms, see Appendix I: Vocabulary, page 66.)

CIT provides Symantec Endpoint Protection for both Windows and Macintosh. This software is free to members of the Cornell community through a university site license.

Protect your personal computers too!

Current faculty, staff, and students can install the Symantec antivirus software on their home computers.

Find out more at www.cit.cornell.edu/services/antivirus.

Enable Your Firewall

All computers connected to the Internet are continuously being probed and scanned for vulnerabilities that might allow a virus, worm, or hacker to cause damage or take control. Firewalls can block unwanted network traffic that you don't need and that could pose a threat. Running a firewall on your desktop or laptop computer is one of the best things you can do to protect your computer. It is just as important as running antivirus software.

Learn how to enable your computer's firewall:

Mac – www.cit.cornell.edu/services/firewall_mac/

Windows – www.cit.cornell.edu/services/firewall_win/

Why should I use a firewall?

Think of writing a book with thousands of pages. What are the chances that the spelling, grammar, and punctuation will be 100 percent correct? Computer software is like hundreds of authors writing a single, very complicated book. Errors (called bugs or vulnerabilities) are invariably introduced. Malicious people spend a lot of time trying to find and exploit these errors to attack your computer for fun or profit, or to cause harm. A properly configured firewall can help block many of these attacks by preventing malicious computers on the Internet from connecting to your computer.

Multi-State Information Sharing and Analysis Center

Set Your Screen to Lock Automatically

Unless your computer is in a secure space that is accessible only by you, you must run a screen saver that will automatically lock your screen after 15 minutes of inactivity and require a password to unlock it. This is necessary to prevent an unauthorized person from being able to see sensitive information or exploit access to your computer in your absence.

For instructions, see Securing Your Computer, Set Your Screen to Lock Automatically (www.cit.cornell.edu/security/howto/index.cfm).

Turn Off Anonymous Access to Your Computer

Your computer must not be configured to allow anonymous access. Allowing people to access your computer anonymously is like leaving your front door wide open!

This means that you may not set up:

- Public folders, where anyone can read and copy files you put there;
- Drop folders, where anyone can leave a file on your computer; or
- Open shares, a folder where anyone can add, delete, or change files.

For information about checking whether there is any anonymous access open on your computer, see www.cit.cornell.edu/security/computer/anon.cfm.

To share files, use the following approved options:

- Departmental file servers can allow you to exchange files with other people in your department. Ask your department's technical support staff if there is a shared departmental file server you can use.
- Cornell Dropbox is a secure mechanism for sharing sensitive files with anyone you conduct Cornell business with, whether they have a NetID or not. See dropbox.cornell.edu.
- Give colleagues you work closely with the ability to access files on your computer by setting up a password-protected folder with a separate username and password for each person. If people only need to retrieve files from your computer, set the folder up so it is read-only.

How to securely share files:

Windows 7 – www.cit.cornell.edu/security/howto/filesharingwin7.cfm

Windows Vista – www.cit.cornell.edu/security/howto/filesharingvista.cfm

Windows XP – www.cit.cornell.edu/security/howto/filesharingXP.cfm

Mac OS 10.5 – www.cit.cornell.edu/security/howto/filesharingmac10_5.cfm#share

Use a Less Privileged Account

When you log into your computer with a username and password, you are using a specific account. The type of account determines what privileges you have on the computer, such as whether you can install new software or change system settings:

- A user account only grants restricted privileges – use this type of account for your daily work.
- An administrator account grants full privileges to make changes – this means your computer is vulnerable to more damage if it's infected by a virus or suffers some other form of attack.

Just as a user account restricts what changes you can make to your computer, it also limits what an attacker can do. Limiting administrator privileges, as a safety measure, may limit the damage from malicious web sites that try to install software without your knowledge, so-called drive-by downloads, see Your browser permits a drive-by download, page 53.

For most people, the need to install software or make other changes to the system is infrequent enough that switching to an administrator account for such tasks should not be a burden. Any inconvenience it may cause is greatly outweighed by the protection you enjoy when using a normal user account.

Depending on the practices of your department, you may already be using a less privileged account. Check with your department's technical support staff to see what your options are and to get help with modifying or setting up accounts.

If you manage your own Windows computer, here is how to modify an account or set up a new one:

Windows 7 – www.cit.cornell.edu/security/howto/useraccountwin7.cfm

Windows Vista – www.cit.cornell.edu/security/howto/useraccountvista.cfm

Windows XP – www.cit.cornell.edu/security/howto/useraccount.cfm

Note: Mac OS X has both Administrator and Standard accounts, but its administrator account does not give the level of privilege that Microsoft Windows does. There is considerably less risk to using an administrator account on the Macintosh.

Lock your computer every time you leave it

Make a habit of locking your computer every time you leave it, so when you are ready to use it again it asks you for your password to log in. This will prevent someone from sneaking on to your computer and stealing files. Follow the instructions for your operating system:

Mac – www.cit.cornell.edu/security/howto/screenlockhowmac.cfm

Windows – www.cit.cornell.edu/security/howto/screenlockhowwin.cfm

Additional Requirements for Computers and Mobile Devices Storing Confidential Data

If your computer holds confidential data, it must be kept secure.

- Any confidential data on a laptop, netbook or other mobile device must be encrypted.
- If your desktop computer is in a location where people could walk up to it, it must be physically secured.

Only authorized individuals should have accounts on a computer that contains confidential data. If this is not the case, the data must be encrypted, so that unauthorized individuals cannot access the data. If you need to encrypt data, check with your department's technical support staff to find out what encryption solutions are recommended.

Escrow your password if you encrypt!

If you encrypt university data, you should not be the only person who knows the password needed to unlock it and you should not use your NetID password for this purpose. Your department should have a process to securely store a copy of the password, so that data can be retrieved should you become incapacitated or forget your password. Otherwise, if something should happen to you, the university will lose access to your work. Check with your department's technical support staff about current practices in your area.

PGP, a no-fee service provided by IT Security, escrows passwords automatically and provides the option for multiple, role-specific key recovery personnel. This ensures simplified access to encrypted data in the event of an emergency. See www.cit.cornell.edu/services/pgp/.

The requirement to escrow the password you use for encryption is University Policy 5.3, Use of Escrowed Encryption Keys (www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/informationtech/encryption.cfm).

The same requirements apply to mobile devices with confidential data stored on them. Smart phones and other portable media such as external hard drives, USB thumb drives, CDs, DVDs, tapes, and diskettes are small and easy to lose, posing a significant risk. If they ever leave a secure location, any confidential data must be encrypted.

See In the News: Viruses on smartphones: Security's new frontier, page 40.

Also see Specific requirements for confidential data, page 28.

Security Precautions for Mobile Devices

You may use a smart phone (like a BlackBerry, Android, iPhone), tablet (like an iPad), or other mobile device. While such devices cannot be secured in the same way as your desktop or laptop computer, you should still take some precautions:

- Avoid keeping confidential data or otherwise sensitive information on a mobile device, because it is more likely to be lost or stolen than a computer, and it is less likely that you'll be able to encrypt your data.

Use strong encryption

The Windows version of Microsoft Office 2007, and later versions, includes a utility for appropriately strong encryption of documents.

The password-protection feature found in Office for the Mac and older versions of Word and Excel for Windows is not sufficient to fulfill the requirement of encrypting confidential data.

If you need to encrypt data, check with your department's technical support staff to find out what encryption solutions they recommend.

- Keep software up to date, since mobile devices are now subject to direct attacks, both from malware (viruses, etc.) specific to a type of mobile device and from attempts to trick people into some desired action. ***Note that mobile devices do not currently enjoy any protections like antivirus software or personal firewalls.***

- Consider setting a password that has to be entered for the device to be used, to keep information safe if the device is lost or stolen. If you use a smart phone, tablet, or the like to check email and you don't have to type in your password every time, then the password is being stored on the device. In this case it's an even better idea that you protect access to your email by setting a good, strong password on the device. ***If someone else gains control of your mobile device, they can both read your email and send messages under your name.***

- If you've set a password for your device, also consider requiring the password be re-entered after a certain period of inactivity. Some devices offer the further measure of erasing your information after someone makes repeated attempts to unlock it using the wrong password.

- Consider what you keep in texts. Even if you don't have a smart phone with Internet capabilities, it may be possible to get important information, or even a new password "texted" to your cell. Be aware that risks apply to all cell phones, not just "smart" ones.

- Be cautious with apps, which can host malware that will expose your passwords, credit card numbers, or anything else you type into your mobile device. To minimize your risks, purchase apps from official app stores (though malware can still slip through vetting) and check online reviews to get a sense of the developer's credibility.

- Turn off Wi-Fi and Bluetooth if you aren't using them. Wireless features can give remote access to hackers who intend to steal your passwords, etc. If you do use Wi-Fi, it should be on a secure network that requires a password for access.

- Back up your data to minimize the chances of losing everything should your device be lost or stolen, or need to be wiped completely due to a virus or other security breach.

- Cornell's ActiveSync service makes it possible for some mobile devices to be wiped or disabled remotely. See Wipe Data from a Lost or Stolen Mobile Device (www.cit.cornell.edu/services/guides/facstaff_email/mobile/wipe.cfm).

- Think very carefully about the risks of letting someone else use your mobile device. They are personal devices, not designed to support multiple users who are protected from each other by individual accounts.

In the News:

Viruses on smartphones: Security's new frontier

By Matt Warman, The Telegraph
February 22, 2010

Mobile phones are the new frontier for cyber criminals, according to the latest research from McAfee. That may sound like a scary headline, but as phones have become more sophisticated, so this new development became inevitable.

Traditionally, cyber criminals have concentrated on the biggest targets, too: so for computers Microsoft has always attracted far more attention than Apple, and on mobile phones Nokia's Symbian OS was hacked most often. Now as Android has finally begun to take Symbian's place and the iPhone's dominance is well established, that operating system too is being examined more closely.

The appeal of mobile phone malware is obvious: these devices increasingly have pin numbers stored as 'contacts', or have people's credit card details stored in iTunes accounts. Hacking is still difficult, but not impossible. Viruses disguised as applications, or links sent from text messages, open up not just financial fraud, but also the possibility of identity theft, too.

More and more people, too, are starting to use their own phones or computers as work devices: that means corporate security is becoming more challenging. Above all else the key is to exert some common sense when using your phone, just as you would with a computer. So don't click on that link or install that app if you don't definitely trust it.

> **Take steps to secure your mobile device**
>
> See Security Precautions for Mobile Devices, page 38.

Read the full article at: www.telegraph.co.uk/technology/news/8311214/Viruses-on-smartphones-securitys-new-frontier.html

CHAPTER 6 Internet Safety

Although computers and online services have become a familiar and ordinary part of our work and daily life, the Internet has many perils.

- If your computer is connected to the Internet, it is under constant attack by criminal enterprises seeking to exploit computing resources to steal information, send spam emails, distribute illicit material, or attack other computers.
- Scam artists attempt to trick you into giving away your money, or giving away information that will let them steal your money.
- Information you post on the Internet and records of sites you have visited can be used for targeted advertising and less savory purposes.

This chapter will help you counter threats like these by explaining how to use the Internet safely:

- Avoid putting your privacy at risk
- Spot fraudulent requests and offers
- Detect a bogus web or email address
- Keep malicious software (malware) from installing on your computer

In addition to the resources provided in this handbook, the **United States Computer Emergency Readiness Team** provides security publications about many relevant topics:

- Recognizing and avoiding email scams
- Spyware
- Virus basics

See these topics and more at: www.us-cert.gov/reading_room

What You Need to Know About Privacy and the Internet

Just as the Internet makes it easy for you to find all sorts of information, you risk others finding out things about you that you don't intend to be public. You may think of sitting in front of a computer as a private experience, but at some level your activity can be traced. There is always the chance that information you send over the network, or store on a network server, could fall into untrustworthy hands.

Never respond to spam

"Never means never. Don't click on an unsubscribe link in a spam message. Don't write to tell a spammer to leave you alone. Don't even use your email program's bounce command to fake out junk senders. When you respond to an unwanted message, you let spammers know that your email address is valid."

MacWorld

As an experiment, see what happens when you search for your name in a search engine. You might be surprised at what appears. If you have a common name, try a search that also includes Cornell, the name of your hometown, or other words that might narrow the search. You should also try different versions of your name.

Web sites you maintain

Any web site you maintain, blog you write, or pages on social networks you set up, like Facebook or MySpace, could give away too much information. You can limit who has access to your information on social networking sites, but people often wind up with a very large circle of "friends," including people you meet in passing or exclusively on the Internet. Not knowing exactly who you are sharing your information with means you could open yourself, or someone close to you, to harassment and threats.

Online information about you can also make it easier for someone to steal your identity, or set you up for some sort of scam. For example, if you write about plans for an upcoming vacation on a blog or social networking site, you could be telling a thief when to burglarize your home.

You are also at the mercy of how well these sites are protected. On several occasions, programming errors have exposed people's information on social networking sites.

Web sites you visit

Where you go and what you do on the Internet today says a lot about where you'll go and what you might do on the Internet tomorrow. Since this is the case, businesses take significant measures to track everything you do while you are using the web. At a minimum, they may be tracking when you arrive, what you click while you are there, and when you leave. When you shop on the Internet, every time you buy something, it's comparable to swiping a customer loyalty card at your favorite store.

Reputable companies make their privacy policy available, and it is worth reading. One common practice to watch for is when a business gives you the option to let "selected" third parties send you valuable offers. This means they are going to sell marketing information about you to other companies. Often, you will need to uncheck a box to opt out.

Market research

Companies, whose business is to understand the needs and wants of consumers, use a variety of market research techniques to do so. Your privacy can be at risk when you participate in surveys, online communities, focus groups, and other types of market research. To participate, you typically enter into an explicit agreement with a research firm, sometimes in exchange for some sort of reward. Reputable market research firms will be upfront about exactly what information they will gather and what they will do with it, and will provide you with a privacy statement.

Say no to market research software (a.k.a spyware)

For some types of market research, the firm needs special software to be installed on your computer to better track your activities. Do not install such market research software on any computer that you also use for Cornell business.

Market research software gives the market research firm and its customers potential access to everything you do on your computer:

- You may be surrendering control of your computer and may not have any way of knowing what information the research firm is gathering about you.
- The software might record not only where you go on the Internet, but also everything you type, including passwords, credit card numbers, and emails.
- If poorly designed, it could break other software on your computer, or make your computer vulnerable to downloads of other more dangerous programs.

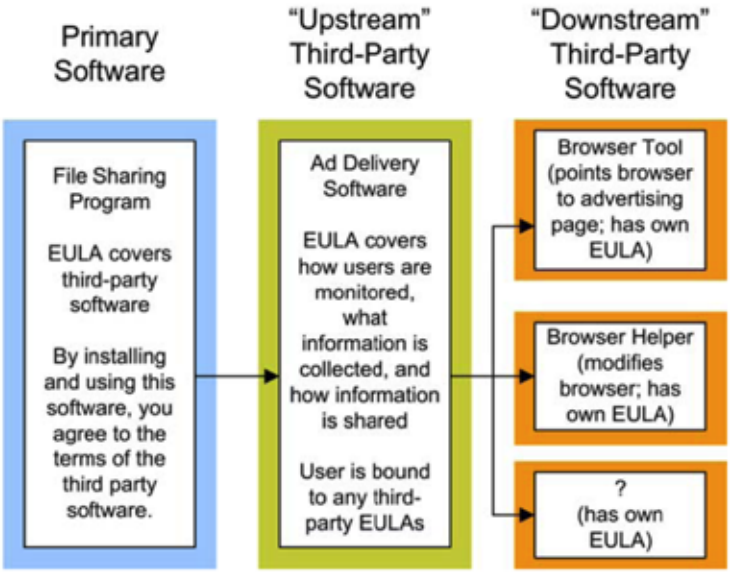
Read the end-user license agreement (EULA)

Be particularly wary if you are asked to install software, even if it appears fairly harmless. And, read the end-user license agreement (EULA – the legal statement that you agree to before you can install the software) to assess their actual intentions. Generally, references to market research in a EULA are a red flag.

The fine print in the EULA will probably grant fairly broad access to your computer and your activities, with surprising latitude in what can be done with the information collected. Because of this, people often refer to market research software as "spyware."

Cascading EULAs are of particular concern; these include EULAs that grant access to a third-party, which in turn can grant access to a third-party, and so on. In this case you could be legally granting access to your computer for multiple unknown parties.

The following diagram, provided by the US Computer Emergency Readiness Team (www.us-cert.gov), illustrates the problem:



For a list of what you can do to protect yourself, download Software License Agreements: Ignore at Your Own Risk, a PDF (www.us-cert.gov/reading_room/EULA.pdf).

Security terms

Adware – software that displays advertisements; you may see popup ads or a small window or bar that displays ads in your browser.

Back door – a means of accessing your computer that bypasses computer security mechanisms.

Bot – short for robot, a computer on which intruders have installed software that lets them secretly control the system from a remote location on the Internet.

Botnet – a network of bots connected via the Internet to perform tasks, such as installing malware, sending spam, or attacking other computers.

Drive-by download – software downloaded by a malicious web site without your knowledge.

Encryption – the process of transforming information to make it unreadable to anyone who doesn't have the password needed to decode it.

Keylogger – software that records everything you type and then sends it off to whomever installed the software.

Peer-to-peer (P2P) – a network of computers that can directly access each other's files.

Phishing – the process of attempting to acquire sensitive information used for identity theft, such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity in an email or instant message, or via a web site or telephone call.

SSL (Secure Sockets Layer) – a method that uses data encryption and digital certificate authentication to secure information traveling over the Internet.

Vulnerability – a weakness in a computer that allows an attacker to make unauthorized changes. Vulnerabilities include weak passwords, poor configuration, or software bugs.

Zombie – a computer that has been compromised, often by a botnet, so that an unauthorized person has complete control to use the computer to perform malicious tasks.

How to Guard Against Internet Fraud

Internet fraud is rampant these days, and becoming more sophisticated. As criminals gain access to more information about people, fraud attempts are being more narrowly targeted.

- You may see fraudulent messages claiming to be from a Cornell office or official, asking you for personal information and passwords.
- Commonly, malicious emails masquerade as invitations to see photos of family or friends, greeting cards, jokes, and pleas for disaster relief assistance.

- Bogus web sites give people a false sense of security by imitating legitimate sites that are used all the time, such as eBay, Amazon, or personal banking sites. Cornell's CUWebLogin page has even been mimicked.

The Internet is a criminal's paradise – a place where anyone can appear to be someone they are not, then disappear without a trace after perpetrating a crime. Don't be a victim. Learn how to guard against Internet fraud.

Don't fall for phishing

Fraudulent, or "phishing," emails try to trick you into replying with information the sender wants, or into visiting a bogus web site. They play on your emotions to try to get you to react without thinking.

- Beware of messages where someone is threatening to close an account or take away privileges unless you provide personal information.
- If an offer seems too good to be true, it probably is.
- Every time you receive a request for personal information (passwords, account numbers, etc.), think about what might happen if you give your information to the wrong person.

These days, with fraud and identity theft such a widespread problem, no reputable institution should be contacting you to solicit personal information in email or over the phone.

AN EXCEPTION: In cases where you contact a trusted service, such as your doctor, it is okay to provide personal information if it is requested. Clearly, there is a difference between when someone contacts you to request information, and when you contact them. For example, when you call your doctor, you may be asked to provide your birth date to verify your identity. This is because your doctor is taking steps to make sure you are who you say you are, to protect the privacy of your personal medical information.

Confirm the source

Confirm the source if you aren't sure whether a request for personal information is legitimate.

Use trusted contact information

- If it appears to be from a Cornell department, contact the department with information you find when you look up its number at www.cornell.edu/search.

  Check the list of Verified Cornell Communications, posted by the IT Security Office, at www.cit.cornell.edu/security/safety/verified.cfm.

  If the email isn't listed on the Verified Cornell Communications page, and you don't get a timely response from the department it purports to be from, contact the CIT HelpDesk for help (phone 607 255-8990, visit 119 Computing and Communications Center, email helpdesk@cornell.edu).

- If it appears to be from a service outside Cornell, such as your bank, PayPal, eBay, or a credit card service, look up their contact information using a trusted source, such as the 800 number on the back of your credit card or the service's official web site. Then call and ask. Or, send a message to the company's customer service via a published address that you find via a trusted search engine.

Look for Extended Validation Certificates (EV Certs)

Verify that a web site you are visiting is who it claims to be. Look for a distinctive color in the address bar of your browser. Green means go! If you see green, the web site has an EV Cert and it's encrypted.

An example of this can be seen at Cornell's CUWebLogin page; to see for yourself, visit any campus service that uses CUWebLogin for authentication, such as the Employee Essentials page (ee.ohr.cornell.edu). Cornell's CUWebLogin page always displays the official Cornell University EV Cert. Click on the certificate name "Cornell University (US)" to view additional info about the certificate.

Firefox's display of Cornell's EV Certificate

Internet Explorer's display of Cornell's EV Certificate

Green EV Certs are more reliable, because a certificate authority has to verify a web site's identity, before an EV Cert will be issued.

EV Certs are harder to fake. When you navigate your browser to a web site that has had its identity verified by a Certificate Authority, such as Verisign or Geotrust, the green color displays in your address bar and you can feel more assured about the trustworthiness of the site.

See www.cabforum.org for a list of extended validation guidelines (steps required before a certificate authority issues an EV Cert), and a current list of Certificate Authority Browser Forum members.

Other clues to look for in your address bar:

- Yellow or red (sometimes accompanied by warning popup windows) – be very cautious. Something in the web site's certificate doesn't match up; it's possible that it expired, or the web site you are visiting has been flagged as a risk.

> "Why are EV Certs more trustworthy?"
>
> Bad guys are good at what they do, so they might create a site called cc.cornell.edu.rr.login, using Cornell's name in the URL and even encrypting the site (thereby showing the color blue, a padlock, or https in the address bar). But a fraudster can't actually prove a real affiliation with Cornell, so getting an EV Cert for a cornell.edu site should be impossible.

- A lack of color – the web site is not encrypted. Look for encryption, and valid certs, on sites where you type your credit card numbers or other confidential information that could put you at risk of identity theft.
- A blue cert, a padlock, or https – the web site has a Secure Socket Layer (SSL) Certificate, which only ensures it's encrypted. Anyone (including fraudsters) can get an SSL Cert to encrypt their web site. That said, regular SSL Certs aren't bad, they just carry a higher risk than sites using EV Certs.

Don't click on email web links

You can also protect yourself by not clicking the web link you find in an email, but instead using a search engine to look up the address for the company's main site, and then navigating to the page you need.

- **CIT's Phish Bowl** provides examples of phishing emails seen on campus, with a particular focus on phishing attempts targeting the larger Cornell community. See www.cit.cornell.edu/security/safety/phishbowl.cfm. The IT Security Office investigates reported phishing attempts; please forward suspect emails to security-services@cornell.edu.
- **Lookstoogoodtobetrue.com** was built to educate consumers, and help keep people from becoming victims of Internet fraud. The web site was developed and is maintained by a joint federal law enforcement and industry task force.
- **Snopes.com** attempts to debunk urban legends – including illegitimate emails that commonly circulate. It can be a good source to check to see if an email you have received is real or an attempt to trick you.
- **Other good sources** like banks and credit card companies usually post examples of scams using their name on their web site, so that people know what to watch out for.

Clues that may indicate that an email is a scam

Beware a false sense of safety. The lack of any of these signs does not guarantee that an email is legitimate!

- The message is poorly written. It may be written with ALL CAPS, have spelling and grammar errors, or it may seem fragmented.
- The message asks you to send personal information, like Social Security, credit card and bank account numbers, passwords, and your date of birth, address, or phone numbers.

- You may see added emphasis, such as exclamation points and words like "immediately," to create a sense of urgency. This is a scare tactic to get you to react.
- The message may have a From line that doesn't make sense.
- A sophisticated phish may include institutional vocabulary, including department names and/or the name of the person who would have sent a legitimate email.
- The message may use a recognizable, but forged, address in the From address. See Forged email addresses, page 50.
- The message may request disaster relief funds or money for another cause that plays on your sympathies.

Watch out for scams trying to steal your money (known as advance-fee fraud or 419 scams)

There are many common email scams circulating that use different country names and variations of the same story to trick you into giving money:

- Someone requesting a small advance of money, in exchange for giving you a big check in the near future.
- An email offering fraudulent opportunities to share in a percentage of millions of dollars, in return for helping a government official, widow, or heir/heiress transfer money from one country to another.

See In the News: Disaster in Japan, relief scams, page 58.

How to understand Internet addresses and detect fakes

One of the best ways you can protect yourself against deception is to check the plausibility of an Internet address. Both web sites and the originating site of an email usually have an address based on the domain name system, a name ending in .com, .gov, .edu, and the like. The first thing you should ask yourself is whether the last part of the name makes sense for the purpose of the site. Would you, for instance, expect to receive a government offer from a site whose name ends in .com instead of .gov?

Sometimes, the site's name will end in a country code. When one of these appears, you need to judge its reasonableness. For example, would your bank be writing you from Romania, or directing you to a web site there?

Use the web address extension to help weigh trustworthiness.

Extension	Description
.gov	*Restricted for government use Note that .gov is the only restricted extension; all the others listed are intended for a purpose, but that doesn't mean they cannot be used for other unrelated purposes.
.edu	Intended for educational use
.org	Intended for individual or organizational use
.com Note that .co.uk is the equivalent of .com in the United Kingdom (Great Britain).	Intended for commercial use
.net	Intended only to be used by network providers
.biz	Intended to be used by businesses
info	Intended for informative web sites
.bz (Belize), .ca (Canada), .cn (China), .de (Germany), .es (Spain), .fi (Finland), .fr (France), .is (Iceland), .it (Italy), .kr (South Korea), .mx (Mexico), .nl (Netherlands), .ro (Romania), .ru (Russia), .to (Tonga), .uk (United Kingdom), .us (United States)	Come across a country code not listed here? Look it up in Wikipedia (www.wikipedia.org), or type it in a seach engine

Even when the site name you see seems plausible, watch for these other signs:

- Concealed web addresses – In web pages or emails, you may find links that say one thing, and link somewhere different.
- Deceptive addresses – Scammers often create deceptive web addresses that resemble legitimate ones.
- Forged email addresses – In emails, the From address is very easy to fake.

Concealed web addresses

A common trick used in fraudulent emails is to create a link that says one thing (mimicking a legitimate web address), and links somewhere different. The same concerns apply to links on a web page, especially advertisements.

For example, here is a link claiming to be from Cornell Webmail (as seen in a phish):

https://www.cornell.edu/webmail/addres_137865476

However, the underlying address was something completely different:

http://www.astromundo.com.mx/Lcons/small/emailchange/

Reading concealed web addresses in Outlook Web Access (OWA)

OWA display's the actual URL a link is leading to, in the bottom left of your browser bar. But, it can be hard to spot if you don't know exactly where to look! The true destination is always tacked on the end, as shown below. In this example, we've crossed out the part that doesn't matter to help you see what you should be looking for (in blue):

~~https://exchange.cornell.edu/owa/redir.aspx?C=f432a3b49429439488e458cfb596b6e0&URL=~~http://www.cit.cornell.edu/services/firewall_mac/

When you hold your mouse over a link in an email message or your browser, it may display the actual URL the link leads to, and may even warn you of a mismatch. Look at the URLs closely to make sure they match and are not mimicking a legitimate address.

Also be cautious of any link that doesn't clearly indicate where it leads, particularly links that say "click here" or links that do not disclose at all where you go when you click them, such as those provided by URL shortening services (tinyURL, bitly, etc.).

Deceptive addresses

Scammers often create a web site name that includes some relevant words, but careful examination reveals it is bogus. This is especially true of web addresses (URLs).

For example, the following URLs are from email messages that purport to come from Cornell:

http://212.100.209.352.8080/cornell/signon.htm

http:// da-us.cornell.edu.nfjje.vg/cornelluniversityonline/CBF.do?CID=705298

You can tell these are bogus links, even though they both contain variations on "Cornell." Ignore everything that comes after the first "/" after http://. What remains is the actual site name:

http://212.100.209.352.8080

The first example doesn't have the host name, just the numeric address (IP address) that underlies a host name. A URL that only includes an IP address should be treated with great suspicion.

http://da-us.cornell.edu.nfjje.vg

The second example includes "cornell.edu," but ends with "nfjje.vg." The ".vg" indicates a site in the British Virgin Islands, an unlikely origin for a message about any Cornell account.

Watch out for simple substitutions. For example, you might also see something like service@cornell.edu, with an "I" (capital i) instead of an "l" in "cornell."

Forged email addresses

It is easy, trivial even, to fake what appears in the From or Reply-to line of an email message. Dig deeper to find the message's true origin.

Sometimes you can easily see other information in the headers (the material that comes before the body of a message) that contradicts the From line. For instance, here are the headers of a message that claims to be from PayPal:

1 → From: "PayPal Customer Service" <service@paypal.com>

Subject: Account Management

Date: Tue, 12 Feb 2008 17:49:19 -0600

X-Original-IP: 131.204.2.2

2 → X-Original-Hostname: d1.duc.auburn.edu

1 The From address looks fine (service@paypal.com).

2 However, the X-Original-Hostname discloses that the message came from somewhere at Auburn University in Alabama (d1.ducaubum.edu).

Look at the message's full headers, for details that normally aren't displayed, to determine whether an email is legitimate. Find out how to reveal full headers in the email software you are using at www.cit.cornell.edu/security/howto/displayheaders.cfm.

Full headers show the path that an email message took in getting to you, and they can be quite long. For example, in a message where you normally see the following:

From: "PayPal"<service@paypal.com>

Subject: PayPal - Security Measures

Date: Tue, 25 Dec 2007 12:30:24 -0600

Turning on full headers reveals the full picture:

Return-Path: <service@paypal.com>

Received: from postoffice7.mail.cornell.edu ([unix socket])

by postoffice7.mail.cornell.edu (Cyrus v2.1.11) with LMTP; Tue, 25 Dec 2007

13:51:10 -0500

Received: from hermes30.mail.cornell.edu (hermes30.mail.cornell.edu [132.236.56.55])

by postoffice7.mail.cornell.edu (8.12.10/8.12.6) with ESMTP id lBPIp7SV004763

for <ewe2@postoffice7.mail.cornell.edu>; Tue, 25 Dec 2007 13:51:07 -0500 (EST)

Received: (from daemon@localhost)

by hermes30.mail.cornell.edu (8.13.6/8.12.6) id lBPIp64G017076

for ewe2@postoffice7.mail.cornell.edu; Tue, 25 Dec 2007 13:51:06 -0500 (EST)

Received: from localhost.localdomain (soapstone1.mail.cornell.edu [128.253.83.143])

Continued...

Continued...

by hermes30.mail.cornell.edu (8.13.6/8.12.6) with ESMTP id lBPIp4F8017044

for <ewe2@cornell.edu>; Tue, 25 Dec 2007 13:51:05 -0500 (EST)

Received: from unknown-host

by soapstone1 with queue (Sophos PureMessage Version 5.301) id 72862194-1

for ewe2@cornell.edu; Tue, 25 Dec 2007 18:41:18 GMT

Received: from router1_tc [10.253.83.144]

by with SMTP id ;

Tue, 25 Dec 2007 18:41:18 GMT

(envelope-from service@paypal.com)

Received: from mail01.crtc.com.tw (unknown [61.30.114.162]) by 128.253.83.144; Tue, 25

Dec 2007 13:41:18 -0500

3 → Received: from dc2 ([12.47.15.100]) by mail01.crtc.com.tw with Microsoft

SMTPSVC(6.0.3790.1830);

Wed, 26 Dec 2007 02:40:44 +0800

X-PH: V4.1@hermes30

From: "PayPal"<service@paypal.com>

Subject: PayPal - Security Measures

Date: Tue, 25 Dec 2007 12:30:24 -0600

And so on…

3 The highlighted information is what you want to check—the first line starting with Received that you find just above the Subject line (bolded). This indicates where the email message started its journey. Look at the host name, mail01.crtc.com.tw. The .tw stands for Taiwan, an unlikely origin for a message from PayPal.

If the email had actually come from PayPal, the Received line would probably show that the email started its journey at paypal.com:

Received: from email-120.paypal.com (email-120.paypal.com [206.165.243.120]) by

128.253.83.155; Thu, 2 Oct 2008 13:05:54 -0400

How Malware Gets on Your Computer

Malicious software, such as viruses, worms, and Trojan horses, collectively known as malware, can end up on your computer via email attachments and drive-by downloads. It can sneak in when you download free software, especially free antivirus software. It lurks in seemingly innocuous ads, and takes advantage of vulnerabilities in peer-to-peer (computer networking) programs.

There is really no guaranteed solution to prevent malware from invading your computer, especially since criminals spend a lot of time keeping ahead of the curve to find new and innovative ways to break down your computer's security defenses.

That said, you can do a lot to guard against malware, such as setting preferences in your web browser to increase security and being cautious about downloading software and clicking links. See Securing Your Computer, page 34, for essential steps you should take to protect your computer from malware.

Your browser permits a drive-by download

A drive-by download is when a malicious web site you visit downloads and installs software without your knowledge. The objective of drive-by downloads is usually to install malware to record what you type and what sites you visit, to search your computer for stored passwords, or to open your computer to remote control. This is currently the most prevalent threat, and one that is hard to guard against.

Drive-by download's are often, though not always, found on sites that could be labeled more promiscuous (gambling, gossip, or other less savory topics). That said, even otherwise legitimate sites can be hijacked into hosting drive-by downloads with third-party ads; Expedia.com and Rhapsody.com both learned this the hard way in 2008. See www.cit.cornell.edu/security/featured.cfm?id=178008.

Drive-by downloads happen in two ways

1. The first appears as an advertising popup or other active portion of a web page. Clicking these popups or, in some cases, even attempting to close them, is interpreted as a consensual download and malware is installed on your computer. Often, in an attempt to trick you into downloading malware, these popups will look like an official warning from your operating system or antivirus software.

2. The second takes advantage of the natural design of your web browser to display web page content. If that content includes something that needs to be downloaded to view it correctly, your browser may offer to run it, infecting your machine.

Google reported, in 2007, one in ten Internet sites hosted a drive-by download. In 2008, Sophos (a major antivirus vendor) estimated that 6,000 newly infected sites appear every day.

Researching addresses more deeply

Sometimes when looking at a URL or at email headers, you will find just a numeric IP address, like 61.30.114.162, and not a host name, like mail01.crtc.com.tw. You can try looking up the IP address with a whois query. One site that does this nicely at no cost is www.domaintools.com.

At the least, you should be able to get information about who owns the address, including the country where it's registered.

Another approach is to enter an IP address or host name in Google or some other search engine. Sometimes the results will reveal a known "bad" site that has been blacklisted.

Reasons why drive-by downloads are so prevalent

- A legitimate web server may have vulnerabilities that allow a hostile site to deliver content.
- Most drive-by downloads exploit the victim's willingness to dismissively click popups and warnings as they navigate to the desired content.
- Very few drive-by downloads can be prevented by keeping software up to date.

How your browser tries to prevent drive-by downloads

Modern browsers take several defensive steps against drive-by downloads. Most will prominently warn of executable programs and offer a safe course of action. Even with these aids, it's important to be wary of any site offering to download or run something you haven't consciously selected.

Some browsers will refuse to directly execute software received while browsing, instead forcing you to save it to your hard drive, to be examined by an antivirus program. When this is the case, if you attempt to run that program later, even after you've finished browsing, you may be prompted with stern warnings about untrustworthy content.

How you can help prevent drive-by downloads

One common configuration makes drive-by downloads particularly effective at introducing hostile software: using the web when you are logged into your computer as an administrator. If you can install software applications, modify your computer's configuration, or perform administrative functions (create accounts, change passwords other than your own, monitor system and network activity, etc.), then you're logged in as an administrator. This means anything run during your web browsing session will have the same privileges on your computer as you do.

Using the web without administrative rights greatly reduces both the risk of a successful drive-by download, as well as the potential damage should one succeed. Learn how to manage administrative rights:

Windows 7 – www.cit.cornell.edu/security/howto/useraccountwin7.cfm

Windows XP – www.cit.cornell.edu/security/howto/useraccount.cfm

Look for https://

Any site asking you to transmit personal information, such as credit card numbers, should always have a URL starting with https:// (note the s), rather than http://. If it does not have the s, what you send over the network is not encrypted. Don't do business there. Of course, just because a site uses encryption does not guarantee it is secure. It's still possible that the entire site is a scam.

You download free software that is actually malware

Before you download software of any type, consider the source. Is this a site you should trust? If you aren't 100-percent certain, do some research. Find a way to confirm the authenticity of the document or application. Ask someone you trust for recommendations. Look it up with a search engine to see what other people have said about the software. Make sure it is safe, and if you are not sure, don't do it!

- Never trust a web page advertisement for free software, especially free antivirus software – it is probably spyware itself. Spyware is software that records and sends off information about you and what you're doing on your computer.
- Avoid clicking on ads, even at trusted sites – they aren't always safe. Often ad space is sold to one party, then resold to a second and third party. In the end, the legitimacy of a site does not vouch for the legitimacy of an ad.
- Be very cautious of running software or opening files from unknown sources, because both can be used as a secret path for malware to be installed on your computer without your knowledge.

See In the News: Movie fans, a prime target for cyber criminals, page 59.

You connect an infected device to your computer

Malware is now commonly spread by devices you plug into your computer's USB (Universal Serial Bus) port. This includes not only thumb drives (also known as flash drives or memory sticks) but also music players, cameras, cell phones, and external drives.

Such malware can infect your computer when you attach an infected USB device. Likewise, USB devices can be infected when they are plugged into an infected computer.

Learn how to protect your Windows computer from USB malware by disabling autorun. See www.cit.cornell.edu/security/howto/autorun.cfm.

An email attachment contains malware

Any time you receive an email with an attachment, ask yourself the following two questions:

1. Who is this email from?
2. Should you be expecting the attached type of information from this person?

If you aren't absolutely sure you trust the sender or you aren't expecting the type of attached information, be cautious. Either contact someone you trust to make sure the attachment is safe, or delete the email without opening the attachment.

Exercise caution with attachments ending in .exe, .cmd, .bat, .scr, .scf, and .pif. You even need to be careful about an attachment that appears to be a Word or Excel document—it might be malware that is masquerading as a legitimate type of file. For that matter, Word and Excel documents can also contain viruses.

Configure your email software so that it only opens attachments when you choose. Don't let your email software automatically open attachments for you.

A peer-to-peer program creates an open door to your computer

Peer-to-peer file sharing allows people to share music, video, and software programs for free, using programs such as BitTorrent.

It is against university policy to run peer-to-peer software on a computer housing confidential data.

Even if you don't have confidential data on your computer, don't install any peer-to-peer software without first checking with your department's technical support staff to find out if it's allowed.

Using peer-to-peer software, even once, could set up your computer to distribute files automatically, which can slow down your computer and network connection, increase your network usage, open your computer up to be compromised, and get you in trouble for copyright violations. Doing it on your work computer puts Cornell's reputation at risk, in addition to your own.

You may not even know that you have peer-to-peer software on your computer, because it is often downloaded by applications and installed on your computer without your knowledge. If you think this may have happened, notify your department's technical support staff, or consult with the CIT HelpDesk (phone 607 255-8990, visit 119 Computing and Communications Center, email helpdesk@cornell.edu)

How to Enhance Your Web Browser's Security (Browser Hardening)

Web browsers have become the primary tool for accessing the Internet. They are used to read news, send email, watch movies, listen to music, chat with friends, make purchases, and manage money. As more and more online tools are built to work within web browsers, they become increasingly complex. This means browsers are subject to more vulnerabilities than ever before. Criminals take advantage of these vulnerabilities to defraud, harass, or exploit people like you.

The measures outlined in this section will help improve the security of your web browser, making your experience on the Internet a safer one.

- Set preferences to ensure software updating is enabled. Internet Explorer and Safari (on MacOS X computers) can be updated through the built-in updater included in the operating system of your computer. Other browsers, such as Firefox, often have automatic updating built in.
- Use the built-in browser security settings. Some web browsers have built-in security settings that can be adjusted to make your browser harder to exploit.
- Disable popups in your browser or install software that will prevent popup windows if your browser cannot block them. Many web sites use popup windows to run malicious software as well as inundate you with unwelcome advertisements.
- (Internet Explorer only) Disable disk caching for encrypted pages to prevent content you view as part of a secure session from inadvertently being stored on your computer, where it can be exposed if your computer is compromised.
- Install add-ons/plug-ins sparingly. Add-ons and plug-ins are applications designed to run within the web browser to provide specific functionality. Examples include Adobe Flash, Apple QuickTime, or the Google Toolbar. Sometimes, you may visit a web site that asks you to install a new add-on or plug-in so you can fully view the web site. This can be risky, as often the web site will direct you to malware, rather than a legitimate add-on/plug-in. When you are sure you want to install an add-on, download it from the original developer when possible to ensure you are getting what you think you are getting.

For directions about how to secure the browser you use, see:

Firefox – www.cit.cornell.edu/security/howto/hardenfirefox.cfm

Safari – www.cit.cornell.edu/security/howto/hardensafari.cfm

Internet Explorer – www.cit.cornell.edu/security/howto/hardenIE.cfm

In the News:

Disaster in Japan, relief scams

By the Cornell IT Security Office
March 16, 2011

Fraudsters prey on tragedy and Japan's 8.9 magnitude earthquake and resulting tsunami are unfortunately no exception.

Mike Lennon, of Security Week, warns "after Hurricane Katrina, the FBI felt it necessary to issue a warning when over 4,500 web sites appeared, all attempting to collect donations to help hurricane victims. The tragic earthquake that struck Haiti in January [also] proved to be an incredible opportunity for scams. Millions of dollars were raised in relief efforts for one of the most deadly natural disasters of all time. Unfortunately, millions of dollars also ended up in the pockets of scammers."

After the Japan earthquake on March 11, fraudulent charity sites were up and running almost instantly:

- New web site domains were registered with keywords that relate to the event, like help, earthquake, japan, tsunami, relief, disaster, fund, and donations.
- Fake donation web sites mimicking the American Red Cross, UNICEF, and other legitimate relief centers will appear.
- Twitter Tweets, Facebook posts, and search engines are already filling the Internet with fraudulent links created by criminals meaning to capitalize on donations.
- A spike in spam emails, with phishing attempts that mimic UNICEF, have already been identified. All direct emails requesting aid, whomever the supposed source, should be considered suspicious.

Watch out for other scams you may come across, which may ask you to download something to view content (you are more likely downloading a virus or keylogger), or which may ask for personal information (name, credit card numbers, etc.):

- "People search" scams offering to find loved ones for a fee
- Variants of the Nigerian scam regarding the "release" of large amounts of money tied up in Japan
- Fake Japanese tsunami video footage circulating on Facebook pages, which leads to a static video image that you have to click on, and which then posts as something you "like" on your wall, thereby spreading itself when others click on it
- Fake YouTube pages, which request a Flash download, and install malware instead

How to protect yourself:

- Delete any unsolicited emails regarding such tragedies. Do not respond to or forward such emails. See the CIT Phish Bowl for fraudulent email examples seen at Cornell (www.cit.cornell.edu/security/safety/phishbowl.cfm)
- Only donate to trusted organizations who already have established channels to receive donations, and are highly unlikely to create new domains for such purposes, such as the American Red Cross (www.redcross.org/) or UNICEF (www.unicef.org/).
- Use trusted news channels for information and video footage of the events.

Read the full article at: www.cit.cornell.edu/services/alert.cfm?id=940

In the News:

Movie fans, a prime target for cyber criminals

Cyber criminals target Harry Potter fans, by KVUE.com
November 18, 2010

Friday's release of the latest Harry Potter movie has cyber criminals working a little magic of their own.

According to online security company PC Tools, the wizard's fans who type "Harry Potter" into search engines are being targeted by identity theives who promise free movie downloads in exchange for personal information.

The sites encourage fans to complete "offers" or register for contests, which require personal information and passwords or possibly malicious downloads, which can lead to identity theft.

Potter fans are encouraged to stick with web sites they know, like harrypotter.warnerbros.com, and stay current on antivirus software.

Read the full article at: www.kvue.com/news/entertainment/Cyber-criminals-target-Harry-Potter-fans-109027214.html

---

Hackers are targeting the new Harry Potter release, by PCTools.com

It has been identified that cybercriminals are continuing to target global events, major news stories and even movie releases such JK Rowling's, "Harry Potter and the Half Blood Prince." Fans are advised to wait until its release in cinemas in mid July (global) or at least download and purchase movies from trusted, legitimate sources.

Cybercriminals are pushing "blackhat" search engine optimization tactics to target the most popular file sharing and P2P networks, including digg.com, blogspot.com and others, pursuing those interested in upcoming movie releases and in particular taking advantage of the sizeable Harry Potter fan base wanting to download the movie in advance of its screening.

First, a user will most likely come across optimized, illegitimate links within the blogosphere. Fans are baited with the text like 'Watch "Harry Potter and the Half-Blood Prince" online free.' Concurrently, comment posts are filled with related keywords to attract more search engines.

This link redirects to a blogspot post that contains more images from the movie itself, convincing the fan that the movie is only one click away. Yet clicking on any one of these links on the blog post redirects fans to the illegitimate video offer.

It is here that fans are prompted to download and install the additional "streamviewer" to view a sneak peek of the film. The streamviewer then proceeds to install malware onto the user's computer.

Be aware that this "streamviewer" tactic is predicted to be used over P2P networks and other file sharing networks as a way of capitalizing on major events, news stories or movie releases.

Read the full article at: www.pctools.com/news/view/id/263/

CHAPTER 7 Working Off Campus

Risk of data exposure or password compromise increases when you use Cornell services, or work with university data, off campus.

- The networks you use are not controlled by Cornell and may be more open.
- A computer and its data are at greater risk of theft when traveling.
- You may not have up-to-date software and full protection when using a computer that's not your own.

This section spells out specific risks and steps you can take to protect your passwords and data while working off campus.

Working on Your Computer at Home

University data stored on a computer you use at home, whether the computer is owned by you or the university, is subject to the same policies as data located on campus. Per university policy, you are the custodian responsible for all Cornell data on any computer you use. See Protecting University Data, page 24, for more information about these responsibilities.

It is your responsibility to know what types of Cornell data you have on your computer at home and to take steps to protect it as outlined here and elsewhere in this security guide.

Use a separate login account

If other members of your household use the same computer, create a separate login account for your Cornell work and data, with a strong password that only you know. Using a separate login ensures other users on your computer cannot view or access your Cornell documents.

Encrypt all confidential data

If you have confidential data on a computer that is located at home, or that comes home with you, that data must be encrypted. Check with your department's technical support staff to find out what encryption solutions are used in your department.

Connect to campus with the Virtual Private Network

Connecting to Cornell's network from home increases the risk of data exposure or password compromise because you have to use networks that are not controlled by Cornell. To minimize these risks, you should use the campus Virtual Private Network (VPN) when working with sensitive Cornell data. This will ensure that everything you do is encrypted as it goes over the network. VPN protects your data from electronic eavesdropping.

To connect to some department and central resources from off campus, you may be required to use VPN. To find out how to install and use VPN, see www.cit.cornell.edu/services/vpn.

Secure your home wireless network

Home wireless networks are easy to set up and extremely convenient to use. However, an insecure wireless environment poses several risks that need to be addressed:

- Anyone near your home can use your Internet connection.
- Anyone near your home may be able to access your computer.
- Anything sent over the wireless connection could be stolen.

The manuals that came with your wireless router should provide detailed information on how to secure your home wireless network. If you no longer have the manual, use the brand name and model type to search for an electronic copy online.

Keep your computer secure

Most of the things discussed in this book apply to your home computers, in addition to your work computers. A very common problem with home computers is having out-of-date operating systems and browsers, as well as not having activated current firewall and antivirus software. Take advantage of your benefit, under Cornell's site license, to install Symantec Endpoint Protection at no charge on your home computer. See www.cit.cornell.edu/security/computer/antivirus.cfm.

If you are working on university business on a computer at home, whether you or Cornell own the computer, you must follow the measures outlined in Securing Your Computer, page 34.

Away from Home and Work

As you prepare to travel, consider where you are going, and what you will be doing while you are there. Ask yourself if there is risk involved with bringing certain types of data along. Take an inventory of the information on your computer, and parse out those things you must have while traveling. If there is any confidential data, it must be encrypted. You might want to consider moving some of the data on your computer to another location temporarily.

Before you leave, make sure there is a backup of your system in case the computer you travel with is lost or stolen.

In addition to the measures described in Securing Your Computer, page 34, the following precautions should be taken when traveling to help keep your data safe and secure.

Connect to campus with Cornell VPN

Working on your laptop while traveling increases the risk of data exposure or password compromise. This is particularly true when using open wired or wireless networks at hotels, airports, and other public places.

To minimize these risks, you should use the campus Virtual Private Network (VPN) when working with sensitive Cornell data. This will ensure that everything you do is encrypted as it goes over the network. VPN protects your data from electronic eavesdropping.

To connect to some department and central resources from off campus, you may be required to use VPN. To find out how to install and use VPN, see www.cit.cornell.edu/services/vpn.

Beware of insecure networks

Treat wireless connections in Internet cafes, hotels, airport lounges, conference facilities, and other public places with extreme caution, because you don't know how safely the network has been configured or who is using it.

The campus Virtual Private Network only protects your connections back to campus, so if you are connecting to non-Cornell sites, like your bank, consider whether you trust that the person or institution providing the network access has adequately addressed security.

Keep your laptop and mobile devices physically secure

- Keep your laptop with you as much as possible.
- When flying, store your laptop in a carry-on bag. Don't check it with your luggage.
- If you leave your laptop at the hotel, lock it in a safe.

- Don't leave your laptop in your car.
- When in a public environment, always keep your laptop with you.
- Travel with a laptop security cable to lock your laptop to a table or chair when you are using it in a public space.

Bring along a laptop without all your data on it

When traveling, if feasible, bring along a laptop that doesn't have all your data on it. Contact your department's technical support staff to find out if they keep spare laptops on hand for this purpose.

Back up your data before you set out

If you have to travel with a computer that has your data on it, make sure it is backed up before you leave. If you lose the computer, this will make it easier for you to recover your data. Backing up regularly not only protects you against losing all your work, but if your computer is lost or stolen, having the backed-up data on hand makes it possible to determine what, if any, sensitive data may be at risk.

Consider encrypting the entire hard disk

If any confidential data is stored on the computer, it must be encrypted. Additionally, if you travel with your computer, it's a very good idea to encrypt the entire hard disk. A benefit of encrypting the entire hard disk is that all of the data on your computer is protected if your computer is lost or stolen, so you don't have to worry about what to encrypt and what not to encrypt.

If you need to encrypt data, check with your department's technical support staff to find out what encryption solutions are used in your department.

Accessing Cornell Services from Other Computers

When you are using a computer that isn't yours, whether it is a public kiosk computer or belongs to someone you know, the risk of data theft is higher.

Consider what data you may be placing at risk when using a computer that can't be trusted, and **do not access confidential data from an untrusted computer**.

I just quickly checked my email. Is it safe?

Time isn't a factor – you only need to type your password, credit card number, or other information once on a compromised computer for it to be stolen.

Public computer kiosks should not be trusted

Always question the security of both the computer and the network. There are many unknowns when using a public computer:

- **How is the computer maintained? Is the software up to date? Have steps been taken to ensure the computer is secure?** Hotels, convention centers, airports, and the like generally outsource technical support services, so you are gambling on the integrity of both the institution's staff and the company providing the service.
- **Who has been on the computer? Have malicious programs been installed? Is someone watching your network traffic?** When you are on a computer you don't own, a keylogger could be recording everything you type. This means you may unknowingly expose your passwords and other information could be stolen even if you are sending them via a secure (https) web session. They will be captured before they go out over the network.

Good practices when surfing the web from a computer you don't trust

Avoid using your NetID and password, and if possible don't access online business or banking services. If you must do either, follow these steps as soon as you have finished.

1. In the browser, clear the cookies, cache, and history before you quit. Find out how to do this at www.cit.cornell.edu/security/howto/clearbrowser.cfm.
2. Exit or quit the browser when you are finished.
3. Change any passwords you used when you are working at a trusted computer again.

In the News:

Mobile apps can create security issues

Excerpts of the article by Phil Hornshaw, Appolicious
October 5, 2010

A few months ago, Citibank (C) notified users of its iPhone mobile app of a potentially huge boo-boo it had made.

The app was saving personal user identification info in a hidden file on the iPhone. The file was completely unprotected, and would sync to the phone owner's computer when the iPhone was plugged in. Basically, if you knew where to look, you could get all the information you needed to access someone's bank account, care of the bank itself.

...Citibank has since corrected the issue with its app. And according to an article from Technology Review, it's not an Apple-only problem.

...For Android users, things are a little safer – but not by much. Apps on the Google (GOOG) operating system don't automatically get to access each other's information, and they are required to ask permission from the user before they access the Internet, write to the phone's SIM card, or access GPS data. But just because an app asks you permission doesn't mean it has to tell you why it's asking permission.

Researchers at Pennsylvania University, Duke University and Intel Labs are working on an app security solution for Android, after they investigated 30 of the system's available apps. They write in the paper about their discoveries that several apps ask for information – like the phone's GPS location, for example – as part of advertising functions. The trouble is, this information is never divulged to the user in the app's license agreement. You're never told you're signing on to give up information about yourself so an app can advertise to you.

...On the Apple side of things, iPhones aren't necessarily more secure than Android-based phones, even though Apple checks each app before it comes to market. The company might be screening its iPhone apps, but it isn't dissecting them – Apple checks their functionality in some pretty basic ways, and if they pass muster, pushes them on to the store. Consider the fact that hundreds of new apps hit the App Store every day, and that they're only delayed by the approval process an average of around six days; there just can't be that much intense checking going on.

So iPhone users may or may not be more secure when it comes to apps, and sleeper agents meant to steal personal information might populate the App Store even now. And while there are some security apps available on the App Store, there's nothing that's the official work of Apple – and if there's one company to trust in this scenario, it's the company that has the most to lose.

For now, both iPhone and Android users should take a common-sense approach to app security: if it seems fishy, don't trust it. That goes for awkward, non-working or low-cost apps. You know: apps that seem like they barely function correctly or not at all. Delete those. They might not work, or only barely work, because their true purpose is to do something else.

...If you still have doubts, consider putting off doing your banking or other sensitive activities from your mobile device unless you have to. A little bit of patience and prevention can be the best medicine for avoiding identity theft.

Read the full article at: www.appolicious.com/tech/articles/3388-mobile-apps-can-create-security-issues

Appendices

I: Vocabulary

Adware – software that displays advertisements; you may see popup ads or a small window or bar that displays ads in your browser.

Back door – a means of accessing your computer that bypasses computer security mechanisms.

Back up (verb) – to copy an electronic record to ensure its information will not be lost, often while compressing data to save space.

Backup (noun) – a copy of an electronic record, maintained to protect the information from loss and often compressed to save space.

Bot – short for robot, a computer on which intruders have installed software that lets them secretly control the system from a remote location on the Internet.

Botnet – a network of bots connected via the Internet to perform tasks, such as installing malware, sending spam, or attacking other computers.

Compromised computer – a computer that cannot be considered secure, because it has been infected with malware, been accessed by someone without authority to access it, or been subject to some other form of malicious attack.

Configure – to choose options in order to create a custom system.

Denial of Service (DoS) – an attack that successfully prevents or impairs the authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim of or participating in the DoS.

Drive-by download – software downloaded by a malicious web site without your knowledge.

Encryption – the process of transforming information to make it unreadable to anyone who doesn't have the password needed to decode it.

Extented Validation Certificate (EV Cert) - A certificate that, prior to being issued, requires verification of a web site's authenticity by a certificate authority. See www.cabforum.org for a list of extended validation guidelines (steps required before a certificate authority issues an EV Cert), and a current list of Certificate Authority Browser Forum members.

Firmware – software that is embedded into hardware; it can be updated and accessed by the user.

Firewall – a security system that uses hardware and/or software mechanisms to prevent unauthorized users from accessing an organization's internal computer network.

Any machine connecting to the Internet should use a firewall. There are two types of firewalls. Software firewalls usually run on computers. Hardware firewalls are separate devices designed to efficiently protect computers. They are usually used by businesses, organizations, schools, and governments. All firewall protection creates a barrier between the computers and the Internet.

Flash drives/thumb drives – very small portable storage devices that may store very large (gigabyte) quantities of information and can be attached to a USB or firewire port quickly and easily to transfer files.

Instant messaging (IM) – the ability to exchange short messages online with coworkers or others. IM solutions can take several forms. They can use an existing Internet-based service, or they can be an Intranet-only solution implemented and controlled within an IT department. The latter is significantly more secure than the former, but lacks access to business partners.

Keylogger – software that records everything you type, then sends it off to whomever installed the software.

Malware – a contraction of "malicious software," malware is a general term used to describe software that infiltrates or damages a computer.

Mobile device (contemporary devices are typically called smart phones or tablets) – a portable device that can be used to perform computer-like tasks, such as browsing the web or reading email, but does not run under a standard desktop operating system, such as Windows, OS X or Linux. This distinction is what makes mobile devices a particular security challenge; standard forms of protection are unavailable or not feasible for general use. The devices typically offer Internet activity through Wi-Fi and/or a telecommunications company data service.

Peer-to-peer (P2P) – a network of computers that can directly access each other's files.

Phishing – the process of attempting to acquire sensitive information used for identity theft, such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an email or instant message, or via a web site or telephone call.

Software patches – fixes to correct a problem. People are constantly finding security holes (vulnerabilities) in computer software that could be used to infect your computer with a virus, spyware, or worse. When vulnerabilities are discovered, the software vendor typically issues a fix (patch) to correct the problem. Patches should be applied as soon as possible because the average time for someone to try to exploit a security hole can be as little as a few days.

Spyware – malware whose principal aim is to surreptitiously collect information by "spying" on the user.

SSL (Secure Sockets Layer) – a method that uses data encryption and digital certificate authentication to secure information traveling over the Internet.

Trojan – malware that appears to perform a benign or useful action but in fact performs a malicious action, such as transmitting a computer virus.

URL (Uniform Resource Locator) – the Internet address on the World Wide Web. It usually begins with http:// followed by the rest of the name of the resource. It is the common name for a site's web page.

Virus – self-replicating malware that attaches itself to a digital document or application, then spreads through copies of that document or application that are shared, frequently via email or USB drives. Viruses almost always corrupt or modify files.

Vulnerability – a weakness in a computer that allows an attacker to make unauthorized changes. Vulnerabilities include weak passwords, poor configuration, or software bugs.

Worm – self-replicating malware that can move from computer to computer on the network. Unlike a virus, it does not need to attach itself to an existing document or application. Worms almost always cause harm to the network, if only by consuming bandwidth.

Zombie – a computer that has been compromised, often by a botnet, so that an unauthorized person has complete control to use the computer to perform malicious tasks.

II: An Overview of University Policies on Computer Security and Data Protection

There are a number of policies that are important to, and inform our use of, information technologies (IT) resources at Cornell. This section outlines the set of policies that are specific to IT.

Data Stewardship and Custodianship (4.12) – Cornell University expects all stewards and custodians of its administrative data to manage, access, and use this data in a manner that is consistent with the university's need for security and confidentiality. Cornell University administrative functional areas must develop and maintain clear and consistent procedures for access to university administrative data, as appropriate.
www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/governance/data.cfm

Responsible Use of Electronic Communications (5.1) – Cornell University expects all members of its community to use electronic communications in a responsible manner. The university may restrict the use of its computers and network systems for electronic communications, in response to complaints presenting evidence of violations of other university policies or codes, or state or federal laws. Specifically, the university reserves the right to limit access to its networks through university-owned or other computers, and to remove or limit access to material posted on university-owned computers.
www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/informationtech/communications.cfm

Security of IT Resources (5.4.1) – Cornell University expects all individuals using IT devices connected to the Cornell network to take appropriate measures to manage the security of those devices.
www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/informationtech/resources.cfm

Reporting Electronic Security Incidents (5.4.2) – Cornell University requires that users of IT devices connected to the University network report all electronic security incidents promptly and to the appropriate party or office.
www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/informationtech/incidents.cfm

Network Registry (5.7) – Cornell University requires network administrators or users to register all devices (including wireless hubs and switches) connected to the university network using a continuously updated central CIT network registry service. At a minimum, the required information maintained in this registry must include the MAC address and IP address, if static, as well as the network electronic identifier (NetID) of the primary user or the person responsible for the administration of the device.
www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/informationtech/network.cfm

Authentication of IT Resources (5.8) – Cornell University owns and manages university electronic identifiers. In the course of its business and missions, it provides its community with access to IT resources, such as email, Internet, and network devices, through these identifiers. To protect these resources from unauthorized use, Cornell requires IT users to obtain electronic identifiers (specifically, Cornell electronic identifiers, as defined herein) to gain access to these resources, and follow specific rules for their use, as well as obtaining, using, changing, and terminating these identifiers. In addition, to avoid unauthorized access to IT resources, holders of Cornell electronic identifiers must follow specific rules for creating and using, and for reporting the suspected compromise of, complex passwords that correspond to a Cornell electronic identifier.
www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/informationtech/authentication.cfm

Privacy of the Network (5.9) – Cornell University recognizes users' reasonable expectations of privacy in information technology (IT) data generated automatically by computer systems and by voice and data network devices. Therefore, the Vice President for IT will disclose IT data only under the following circumstances: (1) in response to a court order or other legal papers, (2) in the investigation of a legal or policy violation, (3) in the event of a health or safety emergency, (4) in specific instances of reasonable requests in the interests of the university, such as collaborative research with other institutions, and (5) to maintain the operation and security of the IT network.
www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/informationtech/privacy.cfm

Security of Electronic Administrative Information (5.10) – Cornell University expects all custodians who have access to and responsibilities for electronic administrative information to manage that information according to the rules regarding storage, disclosure, access, classification of information, and their associated minimum information security and privacy standards, as set forth in this policy.
www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/informationtech/infosecurity.cfm

III References Not Cited in Text

Local Government Cyber Security: Getting Started, U.S. Department of Homeland Security, National Cyber Security Division, and Multi-State Information Sharing and Analysis Center – msisac.cisecurity.org

L.A. County Man Pleads Guilty To Hacking Into Hotel Business Kiosks And Stealing Credit Card Information – www.justice.gov/usao/cac/pressroom/pr2007/161.html

National Cyber Alert System, Cyber Security Tip ST05-010 – www.us-cert.gov/cas/tips/ST05-010.html

National Webcast Initiative, BotNets – msisac.cisecurity.org/webcast/2007-12/

Gartner – gartner.cit.cornell.edu/index.php

5 Steps To Secure Your Smartphone – www.telegraph.co.uk/technology/apple/8311100/Five-tips-to-secure-your-smartphone.html

Acknowledgments

Computer Security at Cornell:
Secure Your Computer On and Off Campus

http://www.cit.cornell.edu/security/

Written and produced by the Cornell IT Security Office
in cooperation with CIT Communication & Outreach.

Original design by Jacqueline Cote-Sherman of Flourish Design.

07/11-PDF