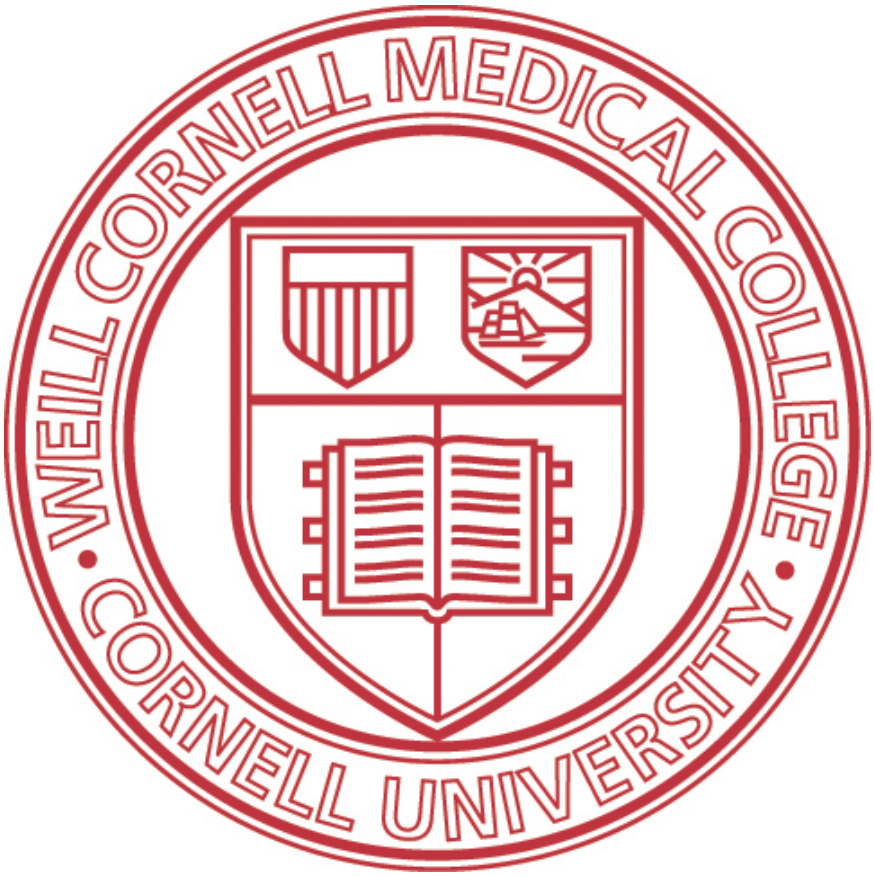


Security for Personal Devices

Best practices for protecting smartphones, personal computers, tablets and other devices from data loss or theft

Information Technologies & Services (ITS) Department

its-training@med.cornell.edu

Updated: December 21, 2016

Weill Cornell Medical College

Table of Contents

I. Use Security Software

The most vital action you can take to keep your computer safe is to install security software that regularly checks for viruses and malicious software (or "malware"). The software you choose should perform regularly scheduled scans for both viruses and malware. Such software will remove any suspicious files and notify you that a threat has been detected.

It's important to purchase and use software from only recognized vendors as fake security software is often sold or given away as part of a scam. Security vendors, such as CrowdStrike, Kaspersky, McAfee, etc. are known and reputable vendors. Software should only be downloaded from reputable websites, including productivity software like Microsoft Office or Adobe Acrobat, as imposters will often entice you to download software that looks real but is actually malicious.

ITS recommends **ClamXav** for computers running Mac OS X, **Microsoft Security Essentials** for computers running Windows 7, and **Windows Defender** for computers running Windows 8 or greater.

Lastly, like most applications, security software requires regular updates. Updates can be in the form of annual license renewals, virus definition updates, or product suite upgrades. Ensure your product subscription is current in order to continue receiving important updates. Security products are updated more often than other products you may be using. This may be as often as a few times a day.

II. Maintain Current Software and Updates

All software should be updated to a supported version, meaning that the vendor is actively maintaining the product and releasing patches. Updates are often released for commonly used products like Adobe Reader, Google Chrome, Mozilla Firefox, Java, and Microsoft Office. These updates should be applied immediately if they contain patches for known security risks. Other updates and upgrades (which may include a brand new release of the product or a brand new operating system) may contain product enhancements. On computers that are tagged and used by Weill Cornell Medicine, ITS discourages applying these non-critical upgrades until we have tested compatibility with other WCM applications.

While most applications will alert you when an update is available, it's important to check vendor websites to confirm the updates are legitimate and safe to apply. It is also necessary to keep the operating systems on your machines up to date. Older operating systems may be unsupported, such as Windows XP. We strongly recommend that you either upgrade your current machine or purchase a new one if you have an unsupported operating system.

Vendors also release updates for applications and operating systems on mobile devices. It's important to regularly install updates from the phone's application store (e.g., App Store, Play Store, etc.) and acknowledge software updates that appear in the phone's "Settings" menu. Regularly updating your devices reduces the risk and threat of a security attack.

To check for and install the latest updates on Windows:

1. Open **Windows Update** by clicking the **Start** button. Type **Update** from the start menu (either in the search box on Windows 7 or from the start screen in Windows 8+), and then, in the list of results, click **Windows Update**.
2. In the left pane, click **Check for updates**, and then wait while Windows looks for the latest updates for your computer.
3. If you see a message telling you that important updates are available, or telling you to review important updates, click the message to view and select the important updates to install.
4. In the list, click the important updates for more information. Select the check boxes for any updates that you want to install, and then click **OK**.
5. Click **Install updates**.

For additional information about automating update installation and for troubleshooting tips on Windows, visit Microsoft's website at http://windows.microsoft.com/en-us/windows/windows-update.

To check for and install the latest updates on Mac OS X:

1. Choose **System Preferences** from the **Apple Menu**.
2. Choose **Software Update** from the **View** menu.
3. Click **Update Now**.
4. Select the items you want to install, then click **Install**.
5. Enter an **Admin** user name and password.
6. After the update is complete, restart the computer if necessary.

For additional information about automating update installation and for troubleshooting tips on Mac OS X, visit Apple's website at https://www.apple.com/softwareupdate/.

III. Password Security

HOW TO SAFEGUARD PASSWORDS

Passwords are used as a primary means of validating your identity in order to gain access to a website, system, or account. The following guidelines will help you safeguard your password:

- Passwords should be kept to yourself; never share them with colleagues, friends, family, or technical support services. No official communication from Weill Cornell Medicine—whether email, phone, or instant message—will ever request your password.
- Use different passwords for work and personal accounts.
- Create passwords that are easy to remember but difficult to guess; never write them down on a sticky note or send them in an email to another individual. You can find more information on strong passwords in the "Simple Techniques for Creating Strong Passwords" Section below.
- Do not let your favorite websites remember your password; although it can be tiresome to repeatedly reenter your password on a website, it limits the chance of an intruder gaining

access to your account. There are alternative services for this such as Last Pass or 1password. ITS will be offering LastPass to all employees for free starting in 2015.

- In the event you feel your password has been compromised, or if you notice suspicious activity from one of your accounts, change your password immediately.

SIMPLE TECHNIQUES FOR CREATING STRONG PASSWORDS

A strong password should contain at least 8 characters and include various types of characters, such as uppercase and lowercase letters, numbers, and special symbols. Creating complex passwords that are difficult to guess can be accomplished by using one of the three methods below:

1. Use a Passphrase

   - Use several characters to construct a phrase that is easy to remember.
   - Abbreviate some of the words to make the phrase harder to guess.
   - Include punctuation to add complexity.

   Example Phrase: "When I was five, I learned how to ride a bike."
   Password: `When I was 5, I learned to ride a bike.`

   Example Phrase: "When I was five, I learned how to ride a bike."
   Password: `WheIwas5,Ilear2ridabik.`

2. Use an Acronym

   - Use the first letter of each word in a phrase to construct a meaningful password.
   - Include punctuation to add complexity.

   Example Phrase: "When I was five, I learned how to ride a bike."
   Password: `WIw5,Ilhwrab.`

3. Use a Secret Code

   - Use the techniques from the passphrase or acronym method to create a strong password, but substitute certain letters for other numbers or symbols.
   - Include punctuation to add complexity.

   Example Phrase: "When I was five, I learned how to ride a bike."
   Password: `WhenIwa$5,Ilh0wt0rab1k3.`

Passwords should also be changed regularly, at least every 3 months for your most sensitive accounts, in order to avoid a compromise.

ENHANCE PASSWORDS WITH TWO FACTOR AUTHENTICATION

Passwords act as one method of authentication, but certain programs and services offer the use of **two factor authentication**. Banks, social media services, and many cloud storage services offer this added layer of protection for free. Two factor authentication typically requires the use of an additional code (sometimes sent via a mobile application or text message) in order to log in to your account. The use of two factor authentication can greatly reduce the risk of your account being compromised even if your password is stolen. Free applications like Google Authenticator and Duo support two factor authentication tokens for logging into many of these services.

USE PASSWORDS ON MOBILE DEVICES

More commonly, smartphones and tablets are being used to access the same services and accounts as laptops and desktops. In addition, mobile devices are much more prone to being lost or stolen. As such, it is recommended to employ passwords and other security measures on smartphones and tablets.

While these features may vary by device manufacturer, most smartphones and tablets support the following functionality from the device's **Security** options in the **Settings** menu:

- **Lock or Timeout** – set this to a reasonable amount of time to lock your device after being idle
- **Passcode** – create a strong (not simple or numeric) passcode that can be used to unlock your device
- **Require Passcode** – a setting that requires your passcode to be entered every time after the device is unlocked
- **Fingerprint Reader** – many phones now have the ability to read your fingerprint to unlock the device. This can serve as an easy log on option if you have a log password.
- **Data Erase** – a functionality that will automatically erase your device after a specified number of failed attempts

While not directly related to password security, many mobile devices offer location services in the event the device is lost or stolen. Applications like Apple's **Find My iPhone** or Google's **Device Manager** allow various remote wipe and alarm commands from a web console for added protection.

USE PASSWORDS ON WIRELESS NETWORKS

When configuring a home wireless router, prevent nosy neighbors and malicious intruders from getting into your private network by applying a password. The setting menus vary based on the device type and your **Internet Service Provider**, but instructions are usually provided. Here are some common tips that will be applicable for all devices and ensure your wireless network is secure:

- Enable **WPA2** security for your Wi-Fi network (this is the highest level of security currently available for wireless networks and is extremely difficult to breach)
- Change the default password on your wireless router (by default, the password to configure your network is simply **password**)
- If available, create a **guest** network that allows access to the Internet for visitors, but prevents them from accessing your personal computers and devices

IV. Don't Leave Your Device Unattended!

Your accounts and passwords grant you access to a lot of information, and sometimes, this information is sensitive or confidential and not meant for other eyes. It's a best practice to log out or **lock your device** when leaving it unattended. Many devices can be configured to do this automatically after a set period of time, but it's best to get in the habit of locking your device immediately rather than allowing a window of opportunity for a malicious individual.

To quickly lock your Windows laptop or desktop:

- Press the ⊞ (Windows) and **L** keys simultaneously, or
- Press the **CTRL**, **ALT**, and **DEL** keys simultaneously and select **Lock**

To quickly lock your Mac OS X laptop or desktop:

- Press the **Control**, **Shift**, and **Eject** (or **Power**) keys simultaneously
- Configure **Hot Corners** from the **System Preferences** that will allow you to lock your screen by moving your mouse to one of the configured corners
- Configure the **Keychain Access** application preferences to show the **lock icon in your Mac OS X Menubar**.

When you leave your devices unattended, you are putting your data at risk and may be held responsible for activity that happens under your account. Always log out and lock your devices when you step away, even for a few moments.

V. Beware of 'Phishing' Emails

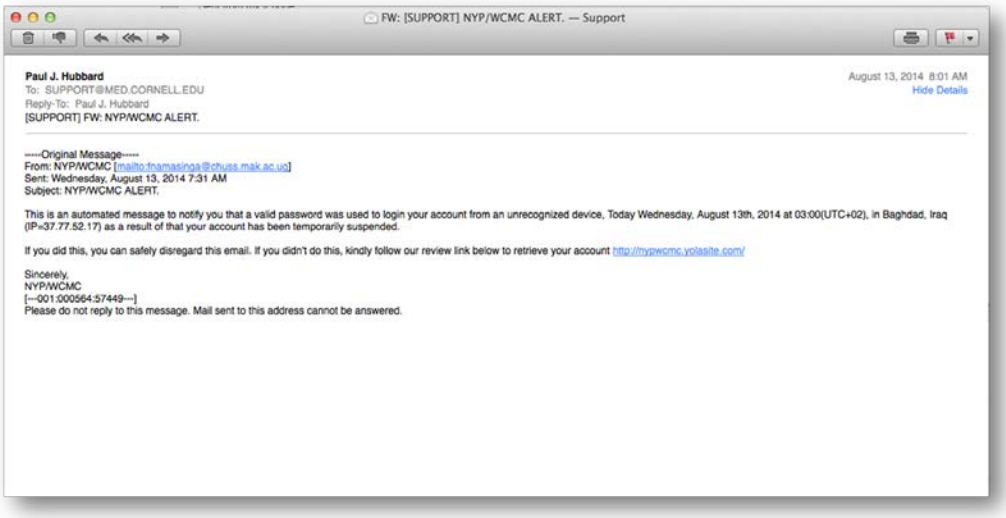
A **phishing** email is an attack in which an attacker sends emails with the intent of tricking recipients into clicking a link or providing sensitive information. These emails usually look suspicious and claim to come from a legitimate company encouraging the victim to take an unsafe action.

If you receive an email from someone you do not know and you are being encouraged to provide a password or any personally identifiable information, **delete the message** and do not respond. If a message comes from a known sender but appears suspicious or contains attachments you are uncertain of, the sender's account may have been compromised. An easy way to determine the source of an email is to hover over this response link. This will display a URL which will usually contain a country where phishing attempts tend to originate from such as Russia or Brazil.

The safest practice to prevent an attack is to avoid opening an email, attachment, or clicking on a link to a bogus website you are not familiar with. If you open anything by accident or provide any information by mistake, run a scan with your security software (described in the first section) and change your passwords to your sensitive accounts immediately.

RECOGNIZING PHISHING EMAILS

The below screenshot is an example of a real phishing email.



There are several key identifiers in this example to indicate the message may be malicious:

- The message is sent from **NYP/WCM**, but the actual address is not a valid @med.cornell.edu or @nyp.org email address
- The message does not contain the appropriate branding or template from the institution
- The message is not signed by an official individual, department, or division
- The website listed is not a valid address

Other identifiers for recognizing phishing emails include:

- Poor grammar, incomplete sentences, or spelling mistakes
- The recipient is being urged to provide money or financial assistance immediately

VI. Handling Confidential Data with Care

Weill Cornell Medicine maintains a formal policy that defines confidential data. Confidential data at WCM includes protected health information, personally identifiable information, student records, financial records, employee records, and research data. While the definition of confidentiality may vary based on your personal data, it's important that you handle confidential data with care.

VIEWING CONFIDENTIAL DATA FROM PUBLIC COMPUTERS

For example, viewing sensitive data on a public computer without logging out of a website or program may make you vulnerable. Many websites employ an inactivity timeout, where your session will be closed after a set period of time. However, in the same sense where it's important to lock your computer when leaving it unattended, it's important to logout of any website when finished.

In addition, when viewing email (either work or personal accounts), be cognizant of saving attachments to your device. Saving attachments to your device could make them accessible to anyone who has access to the computer. Always check the **Downloads** folder on your device to see if any sensitive attachments were saved inadvertently. If you are uncertain about the security of a computer, it's best to limit access to confidential data or sensitive accounts.

VIEWING CONFIDENTIAL DATA ON WIRELESS NETWORKS

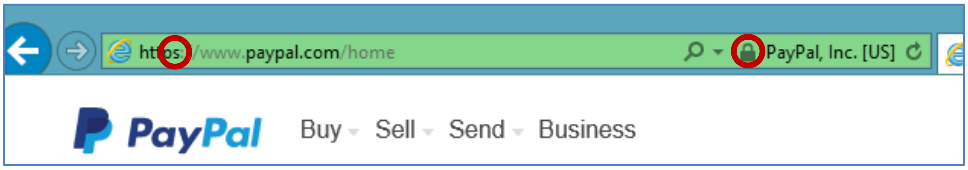
When connecting to wireless networks from laptops, tablets, or smartphones, be wary of connecting to insecure wireless networks. Insecure wireless networks do not require a password upon connection; your device may present a warning about connecting to such a network. Secure networks will require a password to connect, and as such, the amount of users on the network is significantly limited with a lesser chance of an attack. If secure networks are not accessible, it is still appropriate to connect and browse the Internet, but use caution when choosing to access sites with confidential data. Connecting to a WCM VPN connection (Virtual Private Network) will add a layer of security and protection while browsing the Internet. Contact ITS support or visit the SMARTDesk in the WCM Library to get more information about VPN.

CHECKING IF A WEBSITE IS SECURE

Websites that allow or request access to sensitive information are often equipped with a certificate that validates the security of the website. The certificate indicates that a secure connection is in place when transmitting sensitive information across the Internet. This is common for financial institutions, online retail, and other transactional-based services. It provides a level of assurance that you can securely provide your credit card online and know that it is travelling to the company's internal systems with a level of protection.

In order to detect if a website is secured, look for the following indicators:

- https:// in the address bar instead of http://
- a padlock icon



VII. Use Encryption

Encryption is a process which converts plain data into a coded form in order to prevent unauthorized access. When a device is encrypted, a password must be entered in order to unlock (or "decrypt") the device. This is applicable when encryption is applied to computers, smartphones, and tablets.

Weill Cornell Medicine requires all ITS-supported (or "tagged") devices to be encrypted in order to prevent access to confidential data in the event the device is lost or stolen. WCM is utilizing well-known and well-tested encryption products that are native to the operating system (e.g., Microsoft's BitLocker Drive Encryption for Windows devices and Apple's FileVault 2 for Mac OS X devices). WCM also applies policies to smartphones to enforce encryption. Similar encryption techniques can be applied to your personal devices, too.

> Information Technologies & Services will provide encryption to any user upon request for standard hardware and supported operating systems. ITS provides "best effort" support to assist you with encrypting a home computer with BitLocker or FileVault 2 if you will be using your computer for work and accessing confidential data. Contact ITS support or visit the SMARTDesk in the WCM Library for additional information.

Encryption can be applied to an entire computer ("whole disk encryption"), select files or folders, or to removable USB storage drives. WCM utilizes whole disk encryption for maximum security.

VIII. Use Email Securely

When sending information through email, the email message is housed on the recipient's mail server. Email is often available for a long period of time, sometimes indefinitely, so it's best to use email securely and not send confidential information without encryption.

Weill Cornell Medicine is able to ensure that its mail systems are secure, and as such, personal email accounts should not be used for work-related correspondence. Email accounts are provided to faculty, staff, and students for free – contact ITS if you do not have a WCM email account.

When the need arises to send confidential information to a business associate outside of Weill Cornell Medicine, New York-Presbyterian, or its affiliates (such as Columbia University, Rockefeller University, or Memorial Sloan Kettering Cancer Center) it is important to secure the information in order to minimize the likelihood of a data breach. WCM and NYP offer two free encryption services for sending confidential data securely:

- **File Transfer Service (available at https://transfer.med.cornell.edu)**
  - Used to send large or confidential attachments to an intended recipient (whether inside or outside the WCM network).
  - Attachments can be up to 2 GB in size and will be sent with encryption.
  - Recipients can access and reply to the message from a secure interface after creating a free account and password.
  - Requires logging in to the File Transfer Service website to compose the message.
- **#encrypt (available by adding #encrypt to the message subject)**

- Used to send a confidential message or attachment(s) to an intended recipient that is outside the WCM and affiliate network.
- Attachments can be up to 25 MB in size and will be sent with encryption.
- Recipients can access and reply to the message from a secure interface after creating a free account and password.
- Does not require logging in to a separate website; this service can be used from any mail program configured with your WCM account, including your mobile device.

For more information about these services, visit the ITS Security Central page at http://weill.cornell.edu/its/security/.

IX. Use Caution with Cloud Services

Many cloud storage services exist today to provide a means of backing up data, sharing and collaborating with friends and colleagues, and online document editing. Before uploading data to a cloud storage service, ensure the service is reputable and exercise caution when choosing what type of data to upload. Once a file or folder has been uploaded to a cloud storage service, it's extremely difficult to ensure the file is safely removed and deleted from the vendor's servers and backup libraries. While cloud services are generally robust and able to detect malicious attacks, they are still suspectible and your data could be exposed in the event of a breach.

Popular industry leaders include Box, Dropbox, Google Drive, Apple iCloud, and Microsoft OneDrive. Always review the security pages for each service, including the **Privacy Policy** or **Terms and Conditions** documents to understand how your data may be used. Even when using reputable services such as those listed, there is still the possibility that they may lack security features such as string protections for your data. In addition, many of these popular cloud storage services offer additional security by allowing the use of **two factor authentication**, as described in more detail in the **Password Security** section of this document.

WCM has a relationship with Microsoft that will allow our users a free and secure OneDrive account. We are also negotiating with Box though no agreement on secure use has been reached as of this time.