Cornell Cooperative Extension

WSBN IT Training:
PC Maintenance & Security

WSBN IT Staff

Christi Smith, Regional Systems & Support Coordinator

Jenn Matthews, Lead IT Manager

Session Recording

- ***This session will be recorded and available for viewing on Cornell's Video On Demand service***

- *If you have questions and do not wish to be seen or heard on the recording, please enter them into the chat box*

PC Maintenance: Cleaning & Disinfecting

- *The best way to help keep your devices clean is to frequently **wash your hands** with soap and water, especially after using the restroom, eating or whenever visibly soiled.*

- Before cleaning, always turn off device and disconnect from external power

- Resources:
  - https://staff.cce.cornell.edu/units/it/cleaning-and-disinfecting-devices
  - https://www.dell.com/support/kbdoc/en-us/000133659/guidance-for-keeping-your-dell-technologies-equipment-clean
  - https://www.verizon.com/articles/how-to-clean-your-cell-phone/

Cleaning & Disinfecting Do's and Don'ts

- DO:
  - ***WASH YOUR HANDS***
  - Power off and unplug before cleaning
  - Use dry microfiber cloth to remove dust and dirt
  - Use ***damp*** microfiber or lint-free cloth to ***gently*** wipe screen and keyboard
    - Dampen with water or 70% isopropyl alcohol
  - Use compressed air to blow out keyboards, ports
  - Let dry completely before turning on or putting away

- No Clorox or disinfecting wipes
- No 100% alcohol directly on surfaces
- Do not Spray/apply any liquids directly to device
- Do not eat, drink or keep liquids in close proximity to your laptop

- *UV-C devices marketed for disinfecting phones and personal devices have **NOT** been tested for use with your laptops – please do not use these at this time*

OOPS!

Now what do I do?

Best practice for spills on devices:

1. ***TURN IT OFF!*** Immediately turn off, disconnect from power. If your device has a removable battery, remove it, dry and set aside
2. **Turn it upside down over an absorbent surface,** wipe off any visible liquid with a lint-free cloth
3. ***CALL YOUR LOCAL IT***. Notify your local IT or SBN IT staff immediately to ask for next steps.
4. **WAIT. Let dry completely.** Be patient.
5. Once dry, thoroughly clean. Sticky keys can be cleaned with diluted isopropyl alcohol

Image credit - mdbildes/Shutterstock.com

Physical Damage – Warping case, excess heat

Bloated Battery & Decreased Battery

- If your device looks like this, power off, disconnect from power and ***immediately stop using. Call your local IT or SBN IT support for next steps.***

Preventing Battery damage & Extending battery life

- Protect your device from extreme temperatures and condensation
- ***ONLY USE APPROVED CHARGING CABLES***
  - Use the power supply cable provided with your device.
  - If lost or damaged, please contact your IT staff for appropriate replacement
- Don’t leave it plugged in 100% of the time
- Power off device and unplug when not in use for extended period of time

Physical Damage – Screen, keyboard, other hardware

- ***Notify your local or SBN IT staff immediately of any physical damage like cracked screens, damaged keyboards, stuck keys etc.***

  Many newer laptops are covered under ProSupport/Accidental Damage for 3 years.

- For common hardware issues:
  1. **RESTART.** Close all programs, restart.
  2. Shut down, disconnect from power, wait 5 minutes, reconnect power, turn on.
  3. Take notes ***and screenshots*** of any error messages to facilitate troubleshooting with IT staff

Physical Security

- Any CCE or Cornell owned devices should be appropriately secured at all times. This includes:
  - ***Safe storage***
    - Office or home storage should be reasonably secure to protect from theft and accidental damage
  - ***Safe transport in an approved case, bag, or container***
    - Laptop bags should be padded and completely enclose the laptop without applying pressure on the screen
    - Devices transported in cars should not be left out, visible, and unattended.
  - ***Password protected screen lock***
    - Do not disable the screen lock function of laptop
    - Any phone with CCE software ***or email*** is required to have encryption and lock (i.e. pattern, number sequence, biometrics)

When You Walk Away….

- Lock your computer when you walk away!
- Set your computer to go to sleep after a short time in case you forget to lock your computer.

Taking steps to secure your computer not only helps keep your data safe, it keeps all data created, stored, and shared over the network safe.

Physical Security – Safe work spaces

- DO:
  - Stable, solid surface with good ventilation (standing or regular desk, table)
  - Good cable management! Keep those cords safely tucked away to prevent trips, falls, or accidents
  - Keep food and drinks safe distance away, wash hands regularly
  - Regularly clean workspace to remove excess dirt, dust, and anything that can obstruct airflow
  - Ensure setup of workspace doesn't put too much pressure/stress on any cables or ports

- DON'T
  - Use laptop on soft surfaces (i.e. pillows, beds, on your lap)
  - Use in dusty or dirty environments for prolonged periods
  - Cover equipment with paper, fabrics or furnishings or otherwise hinder airflow
  - String power supply cables or networking cords across a space or path

- Ergonomics for the home office (link)

Digital Security – NetID password

- ***Your NetID password should NEVER be used for anything else.***

- Protect your NetID password – never write it down, never share it with anyone. **Literally NO ONE.**

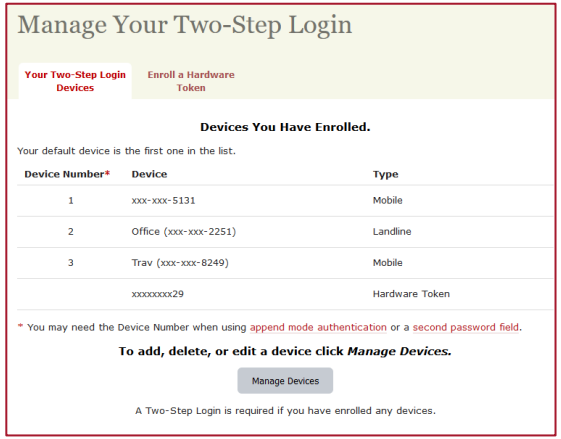
- *If you do get a request for your NetID password, immediately notify your local IT, this is suspicious and could be a phishing attempt*

- Best practice is to change your NetID password whenever you suspect it may have been compromised, or if you've been advised to do so by SBN or campus IT staff
  - https://netid.cornell.edu

Digital Security – Two-step Authentication

- Two-step authentication is now required for most CCE and Cornell services
  - Any login requiring your NetID and password
  - Outlook Web Access (OWA)
  - Microsoft 365 apps – desktop and online access

- Two-step authentication best practices:
  - Register more than one device! https://twostep.netid.cornell.edu
  - Do not save password, or select "remember me for 24 hours" on public networks or personal devices

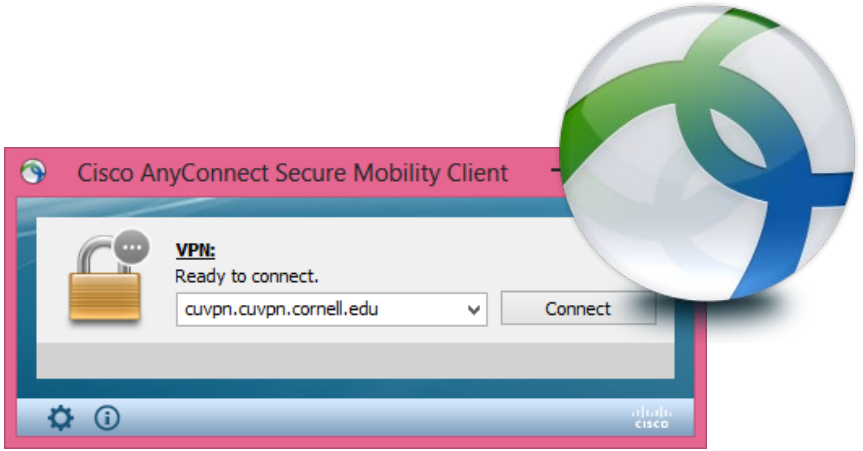


Digital Security – General Practices

- Password management – do not save passwords ***unless*** saved in LastPass
  - Cornell recommends LastPass for secure password management https://it.cornell.edu/password-mgmt
  - Do **NOT** leave passwords written down on, in or near your workspace
- Know your surroundings! Beware of unprotected networks and hotspots
- Disable Bluetooth when not actively using (also extends battery life!)
- Keep your system up-to-date and in good working order
- ***Read all communications from your IT staff***

Internet Safety

- **Use the Cornell VPN** *(Virtual Private Network)* **when working from home, remote office, or traveling**



- Use the VPN when you need to connect to campus resources, such as file servers, print services, the Business Launchpad, Sharepoint team sites, and the CCE Staff site.

- Once connected to the VPN, it provides an added layer of security by sending all of your Cornell-related traffic through an encrypted "tunnel" to campus.

- More information about when you do and don't need to use the VPN:
  - https://it.cornell.edu/cuvpn

Confidential Data & Annual Scans

- IT Policy 5.10 covers confidential data and includes:
  - Social Security numbers
  - Driver's ID
  - Credit card or bank account #
  - Protected health information as defined by HIPAA
- Common examples found on computers:
  - PS404 health insurance form & support documents
  - Personal income taxes, W-2's
  - Retirement or medical paperwork
  - Temporary hire forms
  - Background or DMV check forms
  - Employment, volunteer, leadership applications

Sensitive Data scans are required **at least annually** – some positions (i.e. finance) are recommended to scan more frequently

Spirion/Identity Finder is the scanning software utilized by CCE

For more information:

- Regulated data chart
- https://it.cornell.edu/spirion

Confidential Data – Best Practices

1. Do not store confidential data on your computer.
   Most staff do not have a legitimate business need to collect confidential/sensitive data.
2. Do not **transmit** confidential data via email
   1. If you **must** send confidential data electronically, it can only be sent via Cornell Secure File Transfer
      https://sft.cornell.edu

      More information- https://it.cornell.edu/secure-file-transfer
   2. Once transmitted, the file should be deleted from your computer, recycling bin emptied, and sensitive data scan run on computer ***and your email*** to be sure all copies have been removed
3. If someone sends confidential data to you via email, delete the email, empty trash and scan as above. Recommend notifying sender via new email that ***if that confidential/sensitive data is necessary, should be sent via SFT only***

Virus & Malware Protection

- All CCE owned devices have built in security:
  - Windows Defender & Security Suite
  - CrowdStrike anti-virus and anti-malware

- ***Crowdstrike deployment happening in 2021***
  - *Not sure if you have Crowdstrike yet? Go to Start menu → Virus & Threat protection*
  - Crowdstrike will install on WSBN staff computers after certain conditions are met (connected to Cornell network for period of time, restarted)

PHISHING!

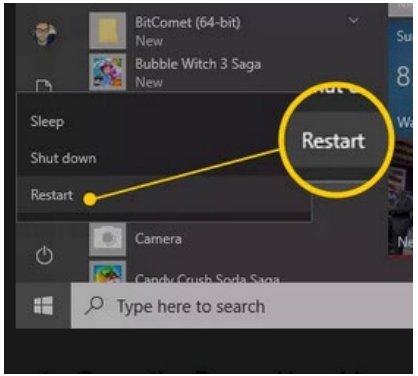
- This is a topic that needs more time than we can devote today ☺

- Resources:
  - Cornell Phish-bowl: https://it.cornell.edu/phish-bowl
  - https://it.cornell.edu/security-and-policy-students/spot-fraudulent-emails-phishing

Best Practices for Optimal Performance

- Shut down your computer when done for the day
  - Windows 10 updates make this process slow – wait ***at least 30 seconds*** after all lights and fan/sounds stop ***before*** closing laptop lid and putting into bag
- Restart your computer **at least once weekly** – may need to do this several times during Patch Week
  - Start/Windows menu → Power → Restart
  - This removes temporary files, installs any updates or patches, and "refreshes" Windows
  - Close all programs and restart **any time computer is running noticeably slower than usual**
- Regularly remove files from Downloads folder and empty Recycling Bin
- If using a laptop, regularly switch things up! Use it on battery power for awhile, use it plugged in and charging.

Updates, updates, updates!



- PATCH TUESDAY
  - 2nd Tuesday of every month
  - Windows, Microsoft security, Microsoft office updates
  - ***RESTART required to complete installation***

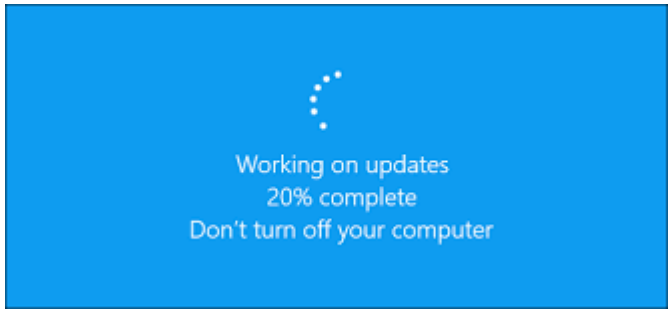
- *Browser & Application updates*
  - Often set to install automatically. Watch for SBN IT news/notifications prompting you to take action if an immediate update is recommended

- Working remotely? Be sure to connect to the VPN regularly for Cornell/CCE licensing and associated updates

Never, ever, ever force a shut down during updates!

- If your computer is installing updates, and you see this screen or an all black screen…

  DO NOT force it to shut down by holding the power button



- Be patient. Take a walk around, find a snack – give it at least 20 minutes.

- If there's still a solid black screen after 20 minutes, with keyboard lights lit but no mouse cursor – contact your local IT or SBN IT staff for next steps. **DO NOT** force a restart unless directed to do so by IT staff

Questions?