




CYBER SAFETY

COLLEGE OF THE CANYONS





RANSOMWARE, VIRUSES, MALWARE
SECURE MOBILE TABLETS
SECURE HOME COMPUTERS
SCAN FOR A VIRUS OR MALWARE
BACKUP DATA
AVOID PHISHING ATTACKS
STAY INFORMED



HOW TO AVOID RANSOMWARE

HOW TO AVOID RANSOMWARE

- Power Down
- Identify threat
- “NO”
- Update software regularly
- Backup

POWER DOWN

The very first thing you should do when you believe you have any computer related intrusion is disconnect from the network and power down your machine. A hard-shutdown is performed by holding the power button down for about 10 seconds to force the computer off. By not allowing malicious software applications to properly shutdown you increase your chances of recovering data. Be sure to close any applications or documents you need to keep prior to a force-shutdown.



POWER DOWN

It's critical to power down your system so you do not infect additional network resources and allow your computer to continue to infect departmental wide resources. Consider manually removing your Ethernet cable to ensure the computer is off-line too.



IDENTIFY THREAT

“Ransomware” holds your data hostage by encrypting your files. It’s on par with locking you out of your house and charging you to buy back the key to get back in. There are many forms of ransomware.

SAY NO

Most Ransomware comes in the form of social engineering via email. The majority of these emails get flagged by our spam filter and never hit your district email. The majority of the attacks you'll be exposed to will be through your personal email. If it looks suspicious and you don't personally know the sender of an email, do not open any related attachments or links. The majority of Ransomware comes in the form of a zipped java applet that contains malicious software. By not un-zipping the document and not opening the program, you're safe. In more unique instances, a compilation of more than one download make up the malicious attack. Again, if it looks suspicious **DO NOT OPEN THE ATTACHMENTS or LINKS.**

UPDATE SOFTWARE REGULARLY

Ransomware tends to exploit out-date software and plugins. Staying on top of your software updates as they become available will reduce the chances of falling victim to an attack.

BACKUP

Your critical documents should be backed up. If it's pertinent to your future self, you should not have one single copy. Most enterprise level network shares are a prime example of a backup. A monthly backup to an external hard-drive, that is not always plugged into your computer, is another option.

ADDITIONAL RESOURCES

[DOJ - How to protect your networks from Ransomware](#)

A decorative graphic on the left side of the slide, consisting of white and light blue lines that resemble a circuit board or data paths. The lines are vertical and horizontal, with some branching out and ending in small circles, creating a stylized, abstract representation of technology or data flow.

HOW TO AVOID A VIRUS

HOW TO AVOID A VIRUS

A computer virus can come in many forms. Deleting, moving, capturing your data is its goal. A viruses will run unwanted processes to either maliciously alter your data or manipulate your computer. Regardless of the intent of a virus, the same principals will keep your computer safe.

- **Run your systems Anti-Virus software regularly**
- **Backup your critical documents to a server or external storage device**
- **Keep your software up to date**
- **Don't open unknown senders email attachments**

<https://www.us-cert.gov/publications/virus-basics>



HOW TO AVOID MALWARE

HOW TO AVOID MALWARE

Malware stands for *Malicious Software*

Malware encompasses many types of Spyware, Adware, and Viruses. Its main goal is to acquire your personal information through keystrokes, network traffic, or screen monitoring. It can simply add annoyance or disable use of your computer and is largely associated with identity theft. Much like a virus, the following will help when dealing with Malware.

- **Backup your critical data regularly to a server or external device** (*expand with HOW TO*)
- **Run Malware detection/removal software**
- **Use caution with unknown senders email attachments**
- **Use caution with unsigned downloads from the internet**

Many spam filters remove the majority of the threats that would usually arise via email. Your personal email should be utilized with more caution than an enterprise email system.

<https://www.consumer.ftc.gov/articles/0011-malware>

A decorative graphic on the left side of the slide, consisting of a vertical column of white lines that branch out horizontally and diagonally, ending in small white circles, resembling a stylized circuit board or data flow diagram.

HOW TO SECURE A MOBILE TABLET

HOW TO SECURE A MOBILE TABLET

Bringing your own device has become more and more prevalent. Understanding the security risks can help secure your information in the event of an accident or theft.

- **Lock your device - assign a password**
Even a four digit numeric password helps
- **Disable critical notifications on the lock screen**
Confidential information can prompt on a *locked screen* of a device and risk leaking unnecessary data.
- **Enable location services**
The ability to erase or locate your device after it has been lost will help ensure your information does not end up in the wrong hands.

Regardless of the event, it's always a good idea to change your email passwords and cloud storage passwords in the event of a loss or theft of a mobile device. This will prevent any *further* damage to your information.

A decorative graphic on the left side of the slide, consisting of a vertical line of light blue circuit traces that branch out into various paths, ending in small circles, resembling a stylized circuit board or data flow diagram.

HOW TO SECURE HOME COMPUTERS

HOW TO SECURE HOME COMPUTERS

There are far too many scenarios to play out with regard to YOUR home. Take a look at these tips to get a grasp on what areas you could give some attention to:

- WPA2 password authentication for your WiFi.
- Do not give out your WiFi password to anyone, either type it in for people, or do not share it.
- Setup a guest wireless network that has restricted access to your home computers
Install anti virus software such as Avast or Norton Anti Virus (pc and mac)
- Enable your firewall settings for your Operating system to prevent unwanted connections.
- Keep your Operating system up to date to ensure the latest security patches are addressed
- Backup your data to a separate device that is not on your network IE: External USB storage
Setup a separate user profile that is not an Administrator Account on your machine
- Use the NON ADMIN account for daily use. Only type in your administrative credentials when prompted and you're 100% sure they're necessary.
- Keep various plugin updates current check out Ninite.com

A decorative graphic on the left side of the slide, consisting of white lines and circles on a blue background, resembling a circuit board or data flow diagram.

HOW TO SCAN FOR A VIRUS OR MALWARE

HOW TO SCAN FOR A VIRUS OR MALWARE

To scan for a virus or malware you need to install a program that can do so.

[WINDOWS DEFENDER](#)

[AVAST](#)

[NORTON](#)

[KAPIRSKY](#)

[MALWARE BYTES](#)

After installing preventative software, it should actively scan incoming data for malicious software. Anti-Virus software will scan both your current files and incoming files for attacks and quarantine the infected files. Some applications also include email protection and will quarantine harmful attachments for you too.



HOW TO BACKUP DATA

HOW TO BACKUP DATA

Backing up your data is the most important preventative approach you should take.

This will help you recover from possible hardware or software issues.

As the life expectancy of a hard drive decreases, the urge to backup your data increases.

It's still the quickest way to recover from a catastrophe.

First check how much data you have.

Then consider how much data you gain over a month or even a year.

Once you've considered how much TOTAL space you're using in a year, triple that number.

Then buy an external hard drive that has at least that much space.

For most people, a 2TB external USB-3 hard drive is enough.

I personally use a 4TB external USB-3 to backup all of my devices critical data.

After you've aligned the hardware with the proper capacity, it's time to pick the backup software.

Backup software is built into Windows and Mac OSX.

The simplest way to get started is to enable the feature for your OS and plug your external hard-drive in once a month to let it backup your computer.

HOW TO BACKUP DATA

Here are some other applications to help you backup to the internet instead of to a hard drive:

[BACKBLAZE](#)

[DROPBOX](#)

https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf

A decorative graphic on the left side of the slide, consisting of white lines and circles on a blue background, resembling a circuit board or data flow diagram.

HOW TO AVOID PHISHING ATTACKS

HOW TO AVOID PHISHING ATTACKS

Email phishing attacks are a form of Social Engineering and can typically be spotted based on the level of detail in the notification. The first cause for concern is usually incorrect grammar or the misuse of a company logo.

- The first action you can take to verify the integrity of a notification is to right-click on the links in the email and select the "Copy Link" option. In some cases you can simply hover over the link and wait for the pop-up preview of the link.
- You can then paste the link into a text editor such as Notepad or TextEdit. Reviewing the link can help you determine the source of the notification. If the link is anything other than a known domain, ie: "apple.com", then you should consider malicious intent.
- Once you have verified the email is indeed spam, delete the email.
- *If you did perform the action requested in the phishing attack email, the first action you should take is to change your password for that account. You can then follow up with your IT department to ensure no further damage has been done.*

<https://www.us-cert.gov/ncas/tips/ST04-014>

STAY INFORMED

US-CERT.gov keeps an active list of threats. Subscribe to their notification system to receive notifications of the latest software vulnerabilities via email.

<https://www.us-cert.gov>