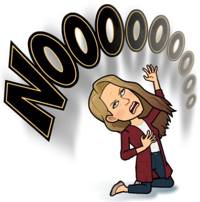
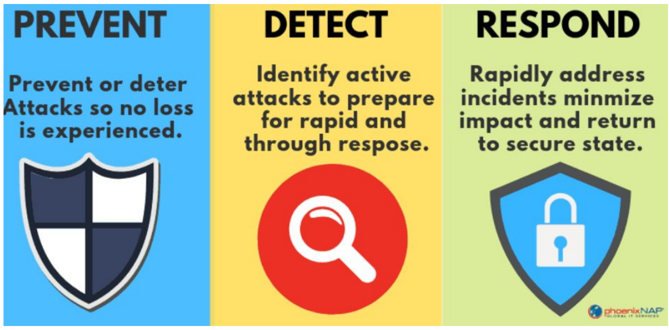
ITRT TECH MINUTE

We thought it would be a great idea to discuss a nasty word: Ransomeware. In order to support your educational needs, teachers have unfiltered access which adds an additional risk to our network. Even though we have IBoss, we can be attacked by user error. It's better to be proactive about IT security and prevent ransomware rather than dealing with encrypted mission-critical files, a request for ransom and system restoration after an attack. For more information: https://phoenixnap.com/blog/preventing-detecting-ransomware-attacks



If you don't want to fall victim to ransomware, you must be proactive or you will end up like the picture on the left. We see a few issues simply by users opening up the email and not realizing whether it is a legitimate email or link from a spear-phishing attack. The following may be indicators that an email is a phishing attempt rather than an authentic communication from the company it appears to be:

- Emails with generic greetings. ...
- Emails requesting personal information. ...
- Emails requesting an urgent response. ...
- Emails with spoofed links.



PREVENT

Prevent or deter Attacks so no loss is experienced.

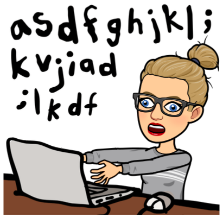
DETECT

Identify active attacks to prepare for rapid and through respose.

RESPOND

Rapidly address incidents minmize impact and return to secure state.

Be aware of where you are connecting to the Internet. Just being something is convenient and you are running out of data, does not mean it is safe for you to connect your device to the WiFi. Sometimes we just want to go into autopilot and connect to anywhere that is available.



Connecting to an outside network makes you susceptible to Ransomware and even can allow other users to easily hack into your personal information.

Similarly, be careful when setting up a hotspot using your phone. Know that it's not a secure connection and that other users can not only see your hotspot but connect to it as well. Check your settings on your phone to make sure your hotspot is password protected.

For more information on securely connecting to various networks see the article below: https://www.pcmag.com/feature/254312/14-tips-for-public-wi-fi-hotspot-security/1

Download Danger!!! While many of us freely download programs and other items to increase our productivity, there is an inherent danger in any type of download. Malware, as well as unwanted programs, are frequently attached surreptitiously to the file you desire to download.

Some common downloads:

- Add-ons
- Browser toolbars and extensions
- Files
- Attachments

As a precaution, you can right-click a file after it has downloaded and run a windows defender virus scan as an extra security precaution.

Keyboard Quick Stop: Did you know...

Rotate Screen: CTRL + ALT + UP/DOWN/LEFT/RIGHT Arrow - We have had to help teachers who have fallen to a prank by students. Now you can fix it. Knowledge is POWER!