County of Los Angeles
lacounty.gov

Security Awareness Tip: Malware

Malware is short for malicious software. It is software developed with the intention of gaining access or causing damage to data, computer or network of computers.

What are some types of Malware?

- **Virus:** viruses attach themselves to files or programs and infect other files. Viruses can be used to steal information, damage a system's functionality, and delete or corrupt files.
- **Trojans:** disguises itself as a normal file or program that has been tampered with. Trojans tends to create backdoors in your security to steal data, install more malware, modify files and monitor user activity.
- **Ransomware:** restricts access to the computer by encrypting files on the hard drive or locking down the computer. Messages are displayed on the computer monitor demanding a ransom to remove the restrictions and regain access to the computer.
- **Spyware:** this malware spies on user activity without their knowledge. It hides in the background and takes notes of online activity including account information, login/password, credit card numbers and more.

How to prevent Malware on your work computer.

- Be aware of phishing emails with attachments or links.
- Hover over links in the body of the email to validate the URL.
- Validate the senders email address if it's from a legitimate company/department.
- When in doubt, seek advice from CEO ITS to verify the validity of the email.

How to prevent Malware on your mobile devices.

- Be aware of suspicious text messaging and emails: Do not click on links or download attachments that you are not expecting.
- Use only official apps: Download official apps from the app stores. Do not install from third party websites.
- Bookmark websites that are important: Bookmarking eliminates typos and prevents opening unwanted websites.
- Keep your device up to date with the latest version of apps and operating system.

How to prevent Malware on your personal computer.

- Be aware of phishing emails with attachments or links and avoid going to malicious websites.
- Install and run anti-malware software and ensure you have the latest security updates.
- Update software and operating systems with latest vulnerability patches.
- Remove legacy programs that are no longer supported or have the ability to download updates.

References:
https://www.zdnet.com/article/what-is-malware-everything-you-need-to-know-about-viruses-trojans-and-malicious-software/
http://www.mysecurityawareness.com/article.php?article=367&title=ways-to-protect-yourself-from-malware#.W9JSVfkrLmE
https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101
http://www.houseofbakchodi.com/malware-definition-and-removal-process/

CEO
Chief Executive Office
COUNTY OF LOS ANGELES