OUCH! June 2025

The Monthly Security Awareness Newsletter for You

Defending Against Malware: The Invisible Enemy

An Innocent Email with Devastating Consequences

Sarah is a talented freelance graphic designer whose creativity and livelihood depends on her trusty laptop. One afternoon, amidst a flurry of project deadlines, she received an email from a prospective client. The subject line read: "Exciting Project Opportunity." The sender's name seemed familiar, perhaps a referral from a previous client. Eager to explore new work, Sarah opened the email to find a polite message outlining a potential project and an email attachment labeled "ProjectBrief.pdf." Without hesitation, she clicked on the attachment, anticipating the details of a new assignment.

Unbeknownst to Sarah, that single click set off a chain of events that would soon disrupt her professional and personal life. The attachment was a cleverly disguised piece of malware, designed to infiltrate her system silently. In the following days, Sarah noticed subtle changes: her laptop's performance deteriorated and applications crashed unexpectedly. She dismissed these issues as typical technical glitches, attributing them to her device's age and heavy usage.

However, the situation soon escalated. When Sarah attempted to log into her online banking to review her checking and savings accounts, only to find out that her password no longer worked. Panic set in as she contacted her bank, only to learn that substantial withdrawals had been made to three foreign accounts. Her savings, painstakingly accumulated over years of hard work, had vanished. Sarah soon realized she had fallen victim to a malware attack that infected her laptop, compromised her financial security, and potentially jeopardized her professional reputation too.

What is Malware?

Malware is a computer program created by cyber-criminals to infiltrate, damage, or control computer systems or mobile devices without your consent or knowledge. The term is a combination of the words "*malicious*" and "*software.*" You have probably heard of viruses, worms, trojans, ransomware, and Spyware. These are all types of malwares.

What makes malware so dangerous is once your computer or device is infected, it can give the cyber-criminal total control without you even knowing it. It can silently capture your activities, including who you are communicating with, what you are saying, and your logins and passwords to your most important accounts.

SANS SECURITY AWARENESS
© SANS Institute 2025

Malware can also silently harvest all your files, including pictures, videos or sensitive documents. It can infect almost any system, smartphones, smart watches, or even smart devices in your home like your thermostat and door locks. Yes, even Apple iPhones and Mac computers can be infected if not secured properly.

Fortifying Your Defenses: Strategies for Protection

Fortunately, there are several simple steps you can take right now to help prevent infection.

1. **Keep Your System Updated**: Regularly update your operating system, applications, and mobile apps to ensure known vulnerabilities are fixed and that you have the latest security features installed. The easiest way to do this is enable automatic updating.
2. **Be Cautious with Emails and Messages**: One of the most common ways cyber-criminals will infect your devices is tricking you into opening an infected attachment, downloading infected software or clicking on a malicious link. Be careful of messages pressuring you into acting right away or something too good to be true.
3. **Use a Strong, Unique Password**: Passwords are the keys to your kingdom. If a cyber-criminal compromises one, they may be able to take over and infect that device or account. Protect all your devices with a unique, strong password or passphrase. Password length is crucial. Whenever possible, enable multi-factor authentication (MFA or 2FA).
4. **Download from Trusted Source**s: Only download software, media, or apps from official or reputable websites. A common way cyber attackers infect mobile devices is tricking you into downloading unauthorized mobile apps designed to take over your device.
5. **Antivirus Software:** When possible, have a trusted antivirus solution installed and set to automatically update. Not all systems or devices can run antivirus, and Anti-Virus cannot catch all malware, but it can help.

Guest Editor

Sherry Peng is currently the Chief Privacy Officer at Agora. She started her career in local government and moved to the private sector after earning her Master's degree in Information Assurance/Cybersecurity. Sherry has worked in the security space for almost a decade and is the current president of WiCyS Colorado.

Resources

The Power of the Passphrase: https://www.sans.org/newsletters/ouch/power-passphrase/
The Power of Password Managers: https://www.sans.org/newsletters/ouch/power-password-managers/
The Power of Updating: https://www.sans.org/newsletters/ouch/power-updating/
Download Danger: How to Outwit Malicious Mobile Apps: https://www.sans.org/newsletters/ouch/download-danger-how-to-outwit-malicious-mobile-apps/

OUCH! Is published by SANS Security Awareness and distributed under the Creative Commons BY-NC-ND 4.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify it. Editorial Board: Phil Hoffman, Leslie Ridout, Princess Young.