CROWDSTRIKE

Smell Something PHISHY?

Phishing is the most successful method used to breach organizations. Phishing is a scam where an attacker impersonates a reputable person or organization with the intent to steal credentials or sensitive information, such as usernames, passwords, credit card details and more. Although email is the most common type of communication used for phishing, the attacker may use a text message or even a voice message in an attempt to gain access.

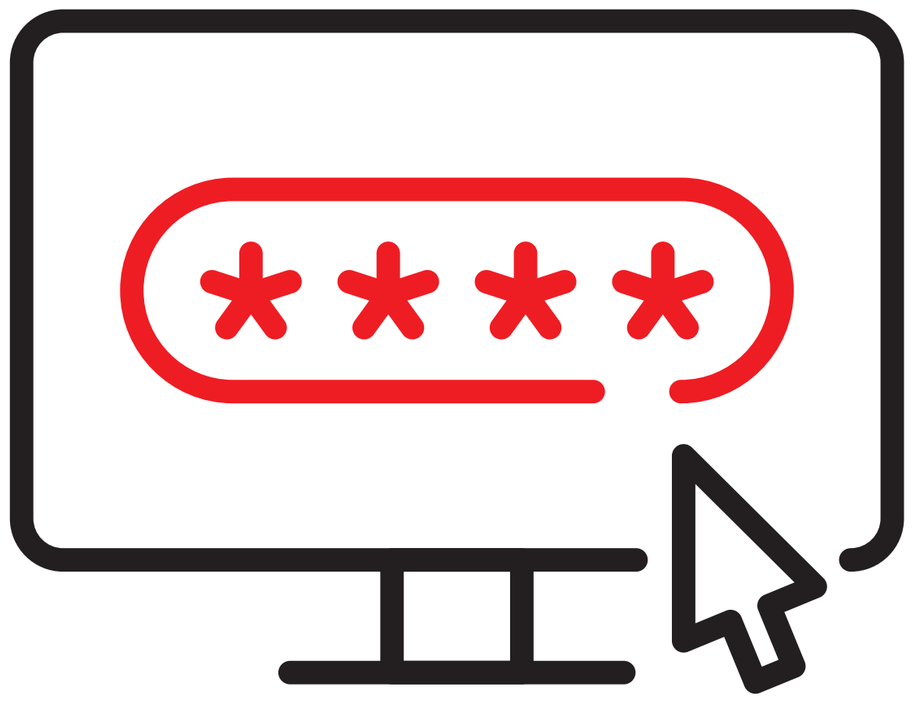
Three tips to fight phishing:

- Do NOT open email attachments or click on links sent by people or addresses you don't know.
- Do NOT provide your personal information to a robocall or in response to an email, and ALWAYS independently verify that the requests are legitimate.
- NEVER send sensitive, confidential or proprietary information over social media, even if the recipient is legitimate and known to you.

Learn More: https://www.crowdstrike.com/solutions/small-business/
Contact Us: (669) 241-1693

Cybersecurity Awareness Month 24
A Security First World

CROWDSTRIKE



How Do I Create a Strong PASSWORD?

Your password protects your identity. Someone using your password can pretend to be “you” and take action in your place, from posting on social media to sending emails to your boss. Passwords are the keys to the kingdom when it comes to your information.

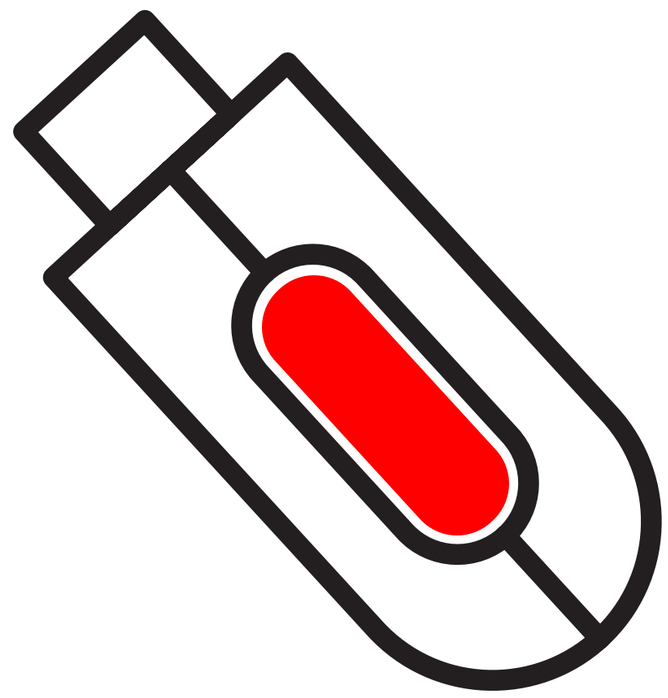
Three critical steps to secure your passwords:

- Use STRONG passwords with at least 15 characters (including uppercase and lowercase letters, numeric digits and special characters).
- ALWAYS protect your identity by enabling multifactor authentication (MFA).
- Do NOT store your password on your computer, on your smartphone or on your desk, and NEVER include passwords in emails.

Learn More: https://www.crowdstrike.com/solutions/small-business/
Contact Us: (669) 241-1693

Cybersecurity Awareness Month 24
A Security First World

CROWDSTRIKE



Lost and Found
THUMB DRIVES

A USB drive may contain malicious software — such as viruses or spyware — that downloads and executes automatically when the drive is connected to your computer.

Three ways to protect yourself from potentially malicious files on USB drives:

- NEVER copy untrusted files from a USB drive or use drives from unknown sources.
- Manually launch files on the USB drive instead of using the computer's AutoRun feature.
- Implement device control, which protects your computer from viruses and malware on USB devices.

Learn More: https://www.crowdstrike.com/solutions/small-business/
Contact Us: (669) 241-1693

CROWDSTRIKE

Watch Out While on Wi-Fi

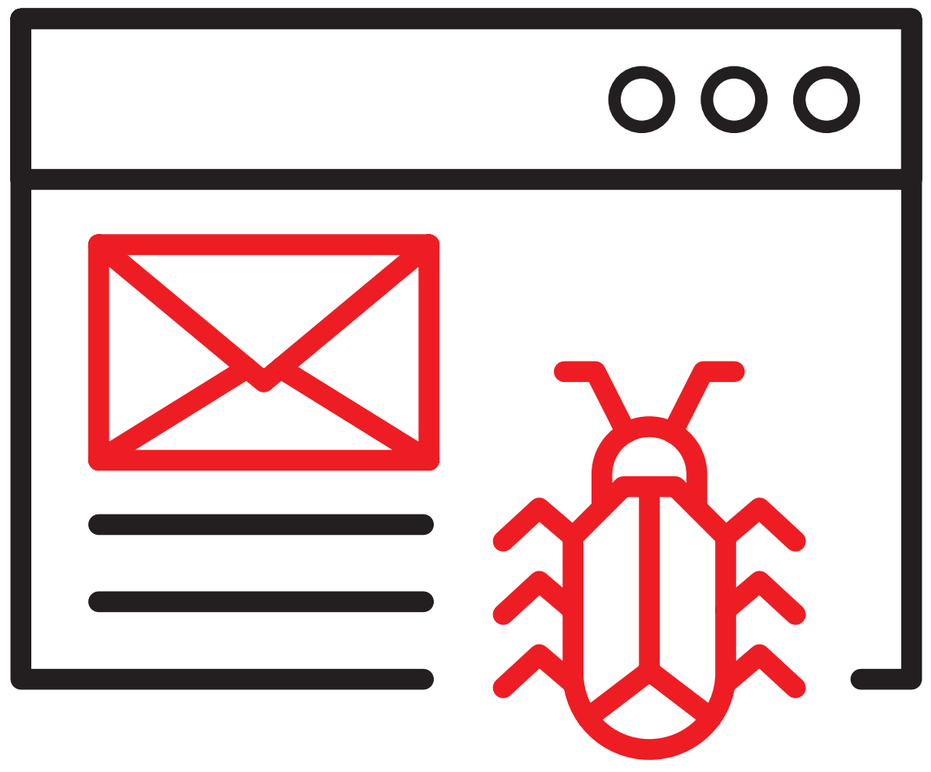
Public Wi-Fi services provide free and convenient access to the internet. However, these networks are often unsecured, and cybercriminals can easily intercept the information you send.

Some safety tips as you surf:

- Disable sharing before connecting to a public Wi-Fi network. Disable the auto-connect feature to ensure that your mobile device does not automatically connect to any available Wi-Fi hotspot.
- Only send information or transact on websites that are fully encrypted.
- Use your mobile device as a secure hotspot wherever possible.

Learn More: https://www.crowdstrike.com/solutions/small-business/
Contact Us: (669) 241-1693

CROWDSTRIKE



Freeware Is MALWARE

Pirated software and freeware can come at a huge hidden cost. They may contain malware — such as viruses and spyware — that will infect your PC when installed. Sometimes, this enables cybercriminals to steal your personal information.

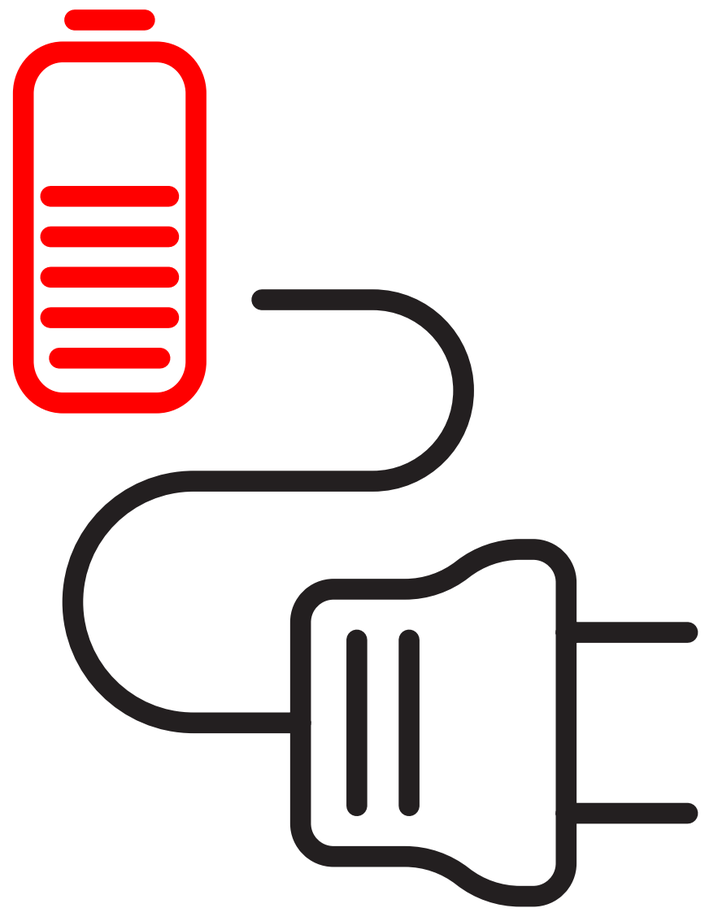
Three tips to keep in mind:

- For legal and security reasons, never use pirated software or videos.
- Do your research and read reviews before downloading freeware to make sure that it does not contain malware.
- Always ask your IT department FIRST if you can install the "free" software or application.

Learn More: https://www.crowdstrike.com/solutions/small-business/
Contact Us: (669) 241-1693

Cybersecurity Awareness Month 24
A Security First World

CROWDSTRIKE



BEWARE of Juice Jacking

"Do I have enough battery power?" For workers on the go, this question is omnipresent. Though airports, hotels and cars now provide convenient options to charge your devices, they may not always be safe. Charging ports give cybercriminals an opportunity to infect your device with malware, take control of your device and even steal your data via your charging cable.

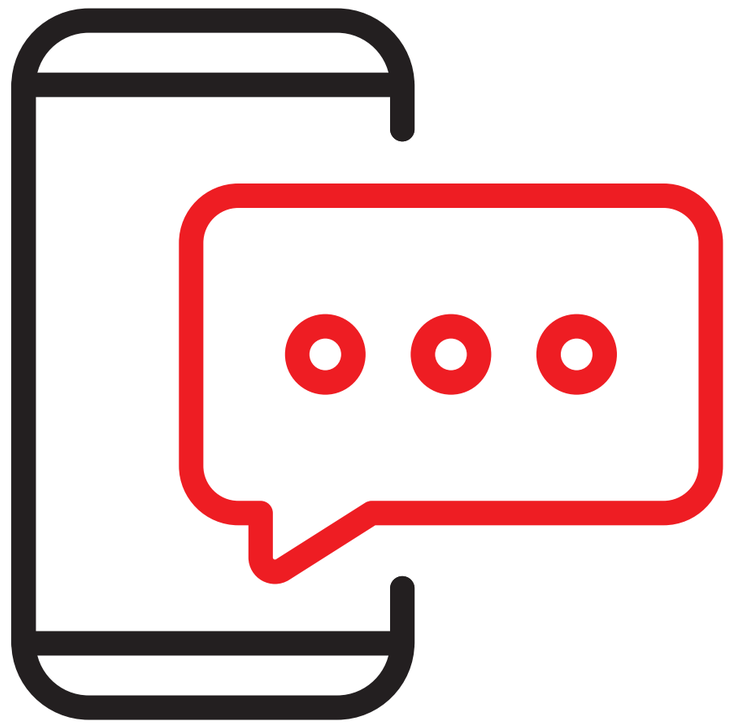
Three habits to practice in public:

- Never use public charging stations.
- Always use the standard power adapter that came with your device and plug it into a power outlet.
- Use a power bank to protect yourself from unnecessary risk.

Learn More: https://www.crowdstrike.com/solutions/small-business/
Contact Us: (669) 241-1693

Cybersecurity Awareness Month 24
A Security First World

CROWDSTRIKE



SMISHING and VISHING

Smishing and vishing are both forms of phishing. Smishing occurs when someone tries to trick you into giving them private information via a text or SMS message. Vishing uses the phone and verbal scams to trick people into doing things they believe are in their best interest. Vishing via phone is often subtle and simple — like receiving a call from "IT" for a common product or service.

Three best practices to stay alert:

- "Trust but verify" should be applied to all correspondence, even when callers identify themselves as reputable or their contact information appears valid.
- Keep control of your equipment and the data on it.
- Inform callers that you don't feel comfortable providing information over the phone, or simply hang up on them.

Learn More: https://www.crowdstrike.com/solutions/small-business/
Contact Us: (669) 241-1693

Cybersecurity Awareness Month 24
A Security First World