Online Safety and Avoiding Scams

Scammers are always trying to separate us from our money. There are as many ways to attempt that as there are scammers. Some very simple steps will help protect your data and identity.

- Keep your device in your control. If you need to leave your device unattended, be sure to lock it up so no one else can use it.
- Choose quality passwords and keep them secure. A password manager can help you maintain strong unique passwords without having to remember them all.
- Enable 2-factor authentication. That extra step when logging in can be a pain, but is worth it to protect your data and identity.
- Be cautious completing quizzes on social media – they are often thinly veiled attempts to gain personal information about users.
- Avoid public WIFI hot spots.
- Review your privacy settings and make sure to log out of public devices after use.
- Keep your software up-to-date. Always install the latest security updates for your devices, ideally by turning on automatic updates for your operating system.
- Back up your data regularly. If you fall victim to a security incident, you will need to erase and re-install the system.

Ransomware

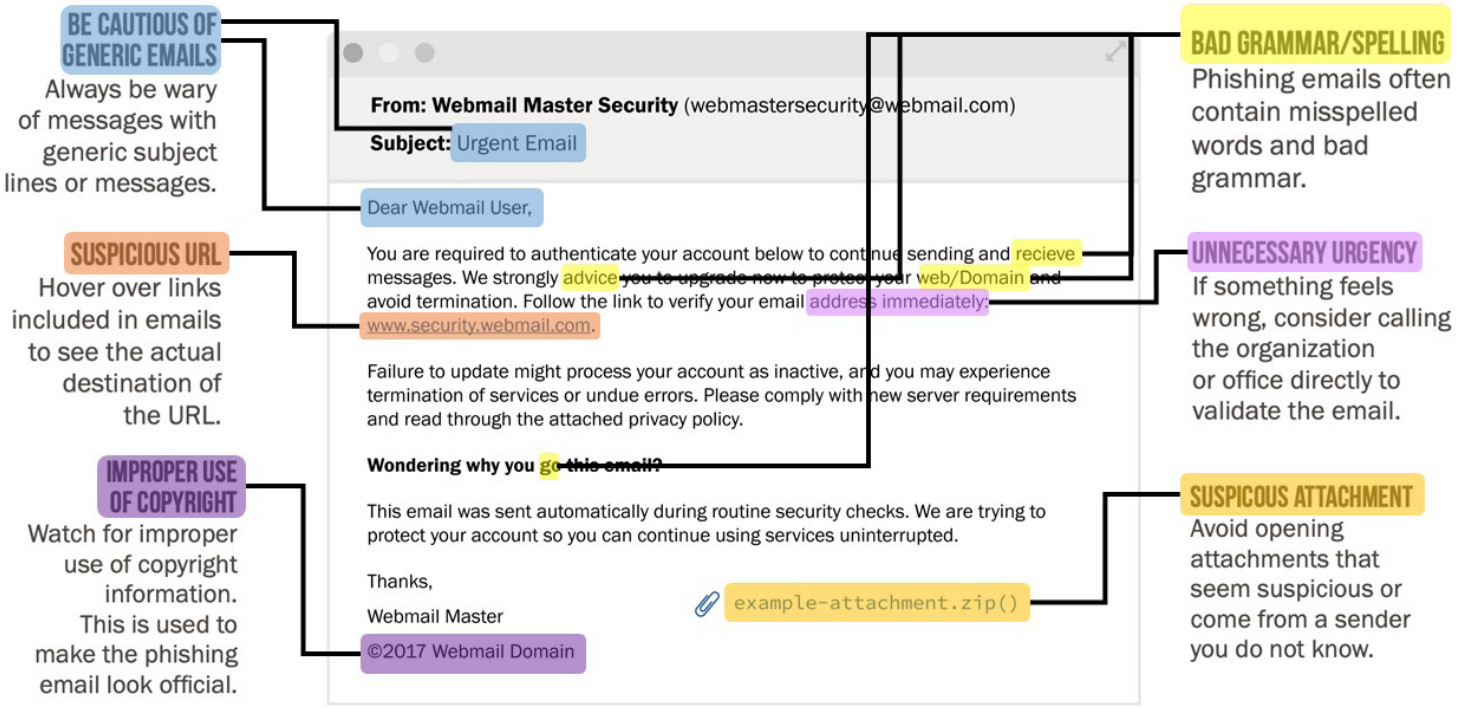
This software stops you from accessing your computer files, system, or network, demanding a ransom for the return of control. You can unknowingly download this malware by opening an attachment, clicking on an ad, following a link, or visiting a webpage that is embedded with the malware. Once it is on your computer, it will lock you out of your files or even the computer itself. Let's talk about some ways to stay safe.

- Keep your operating system, applications, and software up to date. Many times, the patches that are being installed contain security information to help defeat malware.
- Make sure that your anti-virus and anti-malware solutions are up to date and set to update automatically.
- Back up your data and check to make sure that the backup completed properly. Ensure that the backup isn't connected to the computer or the network that you are backing up.

Spoofing/Phishing

Spoofing involves a scammer pretending to be someone that you trust to get sensitive information from you, such as passwords, PINs, and account numbers. They might change a link, email address, or sender name in a small way to trick you into thinking it's someone you know or have done business with. By impersonating someone you may know, like your boss, they can get you to open an email attachment or link that you wouldn't open from just a random email. Using social engineering ploys, scammers will attempt to trick you into sharing personal information or allowing them access to your device. Phishing schemes can be carried out by phone, text, or through email.

- Remember that companies won't generally ask you for your username or password.
- Be cautious of emails with generic subject lines or messages.
- Hover over links included in emails to see the actual destination of the URL.
- Watch out for misspelled words and bad grammar.
- Phishing messages often try to convey a sense of urgency. If you are concerned, consider calling the organization or office directly to validate the message.
- Watch for the improper use of copyright information that is used to make an email look official.
- Never open an email attachment from someone you don't know, and be wary of any unexpected attachments that have been forwarded to you, even from seemingly trusted sources.
- Don't trust the information in the email; search for the company's (or person's) phone number yourself and call to verify the request.



Skimming

Here, scammers attach things like a card reader, keypad, or camera to an ATM or fuel pump to obtain your credit card information number and PIN. Some of these are easy to spot (we will talk about what to look for in a second), but others can be well-hidden. Some are installed on the inside of a fuel pump, and you really won't be able to spot it. It's always preferable to use a pump in a well-lit area that is directly visible to the attendant. These pumps are harder to alter without being seen, as the scammer needs to be able to take a panel off for access. What do we look for?

- Inspect ATMs, fuel pumps, and other point-of-sale machines before use. Look for anything that is loose, crooked, scratched, or damaged. If something doesn't look right, don't use the machine.
- Before you enter your PIN, check the keypad. Pull at the edges to see if it moves at all. A keypad cover may be installed to record your PIN number. Make sure to cover the pad with your other hand to conceal your PIN from a keyhole camera that may have been installed.
- Use debit and credit cards that have a chip. In the United States, it is more common to find a machine that steals your information from the magnetic strip than the chip.
- If the machine won't give your card back when the transaction is done or canceled, call your financial institution. Make sure that you use the number from the institution's app or website; don't use any information that is posted on the machine.