Be cyber smart: Get your "Shields Up"
Simple Steps for Safety Online

Cyber scams are nothing new. Every day, hackers and other cyber criminals are looking for the easiest target online. Do you think you're not worth being the target of online predators? Think again!

Whether it's your identity, your bank account information, or simply what's in your email, your information is valuable and cyber criminals will do whatever they can to access it. They're counting on you thinking you're not a target. It's time to get your ***Shields Up*** and take steps to prevent yourself from becoming the victim of a cyber crime.

Let's start with the basics of cyber hygiene-- easy and common-sense ways to protect yourself online. Here are the four easy things you can do today to keep yourself cyber safe:

- **Use more than one type of authentication on all your accounts.** A password isn't enough to keep you safe online. By implementing a second layer of identification, such as a confirmation text message, a code from an authentication app, face or fingerprint verification, or a security key, you're giving your bank, email provider, or any other site you're logging into an extra layer of security. Multi-factor authentication can make you up to 99% less likely to get hacked or have your information stolen!
- **Update your software.** Hackers will try to exploit software flaws and vulnerabilities. Update the system software on all your devices, such as mobile phones, tablets, and laptops. Make sure to also check for updates your applications regularly – especially the web browsers – on all your devices too. Make it easy for yourself by simply turning on automatic updates for all devices, apps, and operating systems.
- **Think before you click.** More than 90% of successful cyber attacks start when you click an unfamiliar link in phishing email. A phishing scheme is when a link or webpage looks legitimate, but it's a trick designed to have you reveal your passwords, credit card numbers, or other sensitive information. In addition, phishing emails may be attempts to try to get you to run malicious software, also known as malware. If it's a link you don't recognize, trust your instincts, and think before you click.
- **Use strong passwords.** A strong password should be eight or more characters utilizing a combination of letters, numbers, and special characters. Avoid using the same password on different accounts. Ideally, individuals should also use a password manager to generate and store unique passwords.

Our world is increasingly digital and increasingly interconnected, and we all have a responsibility to truly protect the computer networks we all rely on. Become a champion for cybersecurity and share these tips with your friends, family, and neighbors.

For more, information visit CISA's Shields Up webpage.