What You Need to Know About Cybersecurity

From deceiving users into disclosing personal information to compromising entire information technology networks, it seems cybercriminals will use any means to reach their goals. Attackers can potentially steal identities, medical records and more, but, most commonly, they have financial motives.

In the past 10 years, the number of cyberattacks on organizations has grown and become more sophisticated. Attackers, in general, have unlimited targets — whether it's an individual or business computer, computer network, system or infrastructure.

Cybercriminals can launch attacks utilizing diverse methods, including the following more prevalent examples:

- **Phishing** is an email scam attempting to coax recipients into sharing personal or financial information. Phishers often use counterfeit websites or email messages that appear to be from a trusted individual, organization or brand in order to steal important information, such as usernames, passwords, credit card numbers or social security numbers.
- **Malware**, or malicious software, is computer code or software with intent to harm. It can describe a number of different types of attacks, including viruses, Trojan horses, worms, ransomware, spyware and more. Often, this type of attack enters a computer not up to date on its "patches" or software updates, or in a downloaded attachment or software. These attacks have the capability to cause serious damage, whether stealing information or taking down a computer system. In the case of ransomware, the attacker encrypts files, demanding a ransom to release them.
- **Password attacks** are when a cybercriminal tries to decipher a user's password to break into a computer system, often by using software on their own system.

To prevent cyberattacks, users should be mindful of cyber interactions. Here are additional tips:

- Avoid opening unexpected email attachments, even if the message is from a trusted sender.
- Never respond to online requests for personally identifiable information. Most organizations will not ask for this information through the Internet.
- Modify your passwords on a regular basis.
- Ensure your home computer always has the latest software updates installed and also has antivirus software installed and running.

- When in doubt, trust your instincts. If an offer looks bogus, it likely is.

For more information on cybersecurity and additional tips to protect yourself, visit the Department of Homeland Security's cyber incident webpage.