

CyberSecurity Corner – Ways To Prevent a Phishing Attack

- 1. Be careful and think twice:** Don't trust every email you get, especially if it asks for personal information or tries to scare you into acting fast. Take a moment to look closely at the email and think about whether it seems real or not.
- 2. Check the sender:** Look at the email address and see if it looks legitimate. Sometimes, scammers use tricky spellings or fake names to make their emails seem real. Before you click on any links, hover your mouse over them to see where they really go.
- 3. Watch out for attachments:** Don't open any files that come from unknown people or seem suspicious, even if they say they're important. They could have viruses or malware that can harm your computer or phone.
- 4. Use two-factor authentication (2FA):** This is an extra security step you can add to your accounts. It usually means you have to enter a special code or approve login attempts from a trusted device or app. It makes it much harder for hackers to get into your accounts
- 5. Educate yourself:** Learn about the latest phishing tricks and how to spot them. Many websites and companies offer tips on how to stay safe online. Keep up to date with their advice so you can protect yourself better.
- 6. Get good security software:** Install a good antivirus program and keep it updated. It will help find and remove any bad stuff on your devices.

7. Report phishing attempts: If you get a phishing email, tell the right people about it, like your bank or the company the email pretends to be from. This helps them catch the bad guys and stop them from tricking others.