# Security Tips Newsletter

2026 | Issue No. 3

## Security is Everyone's Responsibility

***Be cyber smart to stay cyber safe.***

**What's in this Month's Cyber-Tips Newsletter?**

### How to prepare for AI-Powered Security threats.

AI has many uses (write letters, summarize documents, assist in program coding, etc.), one that has many concerned is its ability to create malicious emails (Phishing). The ability to identify malicious emails via grammatical errors has been greatly reduced with the use of AI. It also enhances the content of the malicious emails to make it more believable because of the search of the Internet for information pertaining to you (Facebook, Instagram, etc.).

---

You can take steps to protect yourself from being a victim of these malicious emails.

1. **Always question an email** – Question what you see in an email or other communication channels (text, voice, etc.). Phishing accounts for 74% of the social engineering attacks.
    a. Is this a normal request?
    b. Is it using normal communication channels? For example, would the police be sending you a text message?
    c. Is there a sense of urgency?
    d. Does the email include/request a money exchange? For example, money has been deposited into your account by mistake or the purchase of bitcoin/gift cards.
2. **Question content in media (Deepfake)** – AI has the capability to create highly realistic media (video, photos or audio) impersonating a person's likeness or voice. Deepfakes are getting harder to identify with the improvement of AI. Below are some warning signs to assist in identifying.
    a. Sense of urgency
    b. Suspicious links
    c. Requests for money or sensitive information
    d. Emotional pressure
    e. Sense of secrecy
    f. Is this a normal request?

    ***Tip:*** *A good way to protect your family is to create a code to use when you doubt the legitimacy of a call.*
3. **Safe Internet browsing** – Be cautious when browsing the Internet. Think before you click on links. Take time to review to see if the link is correct. Be cautious before clicking on "Sponsored content". Malicious actors can pay to have their content at the top of the search.
    ***Tip****: It is recommended to scroll down to the link for the actual site you are searching for.*

4. **Spoofed Calls –** Malicious actors will call you and change the caller ID number that is shown on your phone to match the organization's (Bank, court, police, etc.) phone number they are impersonating. These calls will use a sense of urgency to get you to complete a task. The task will be some form of money transfer using bitcoin or gift cards. Ask yourself, is this a normal request? Would the police call you and request you pay a fine over the phone? If you doubt who the caller is, let them know you are going to hang up and call back at a known phone number.
   ***Tip:*** *Do not call back a number they give you. Look up the number from another source (Internet, bank statement, etc.) and then call the number you found.*

   a. Is this a normal request?
   b. Is it using normal communication channels? For example, would the police be sending you a text message?
   c. Is there a sense of urgency?
   d. Does the email include/request a money exchange? For example, money has been deposited into your account by mistake or purchase of bitcoin/gift cards.

***Be safe and Think before you click/take action!!!***