AVOID EMAIL (PHISHING) SCAMS

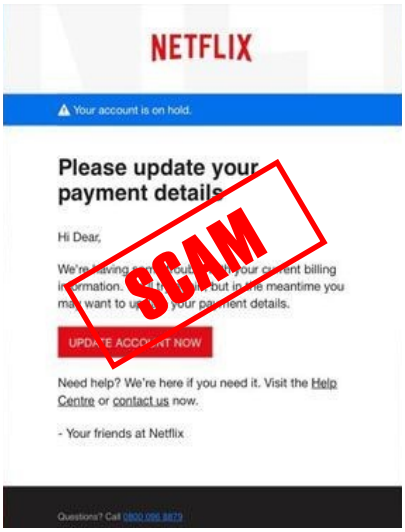
Email and text scams cost people over $57 million a year. So, the more you know, the better you can protect yourself.

Scammers use calls, emails, and text messages to attempt to steal passwords, debit/credit card numbers, account numbers, and social security numbers.

Phishing emails and texts look like they are from a company that you recognize and trust. The message may look like it is from a bank, credit card company, online store or a social networking site. The message usually tempts you to into clicking on a link or opening an attachment. The message may say there's a problem with your account, include a fake invoice, offer a coupon, or ask you to confirm payment/personal information.

Signs of a phishing email scam:

1. The sender's email address doesn't match the name of the company.
2. The information has an "urgent" call for you to take some sort of action.
3. The email has a generic greeting e.g. "Hi Dear,".
4. There are usually grammar and spelling errors.
5. If you hover over the link information (**without** clicking), it doesn't match the company name or information.



Protect yourself.

1. Make sure your computer software will update automatically.
2. Protect your phone by setting it to update software automatically.
3. Safeguard your accounts by using multifactor authentication. This will require more than one set of credentials to log in to your account.
4. Back up your information and data on a device not normally connected to your home wifi connection. We suggest an external hard drive.
5. Don't click on any links of unsolicited emails or texts.
6. NEVER share personal information via unsolicited emails, texts, or phone calls.
7. Verify any potential account freezes/locks/issues/free offers by contacting the company directly via their verified home page, your normal log in process, or by calling the phone number on their site.

We're happy to help!

We are your advocate. Here to help you prevent fraud on your account. If ever in doubt, call us before responding to an email, text, or call. Our trained staff can give you information on steps to protect yourself and your funds.

Remember, if it seems "phishy" it probably is. It is always better to be safe than sorry when it comes to protecting your personal information and your financial accounts.