Your online security and privacy are important to us. We want to remind you of an increasingly common form of cyber-attack - phishing. Phishing attacks are widespread and we do not want you to be victimized.

Phishing is the fraudulent practice of sending emails that appear to be from a reputable company with the goal of getting you to share sensitive information. Often, the targeted information includes login credentials, credit card information, bank account details, or other personal information.

Spear-phishing is a highly targeted form of phishing. Unlike a general phishing attack that casts a very wide net (sending generic, mass emails), a spear-phishing attack is personalized with specific details about the message's recipient.

Spear-phishing attackers may gather personal information from your social media accounts or the dark web to create messages that appear to come from trusted sources - like companies or even individuals that you know. They use these personal details to trick you into taking an action that could cause you to share even more personal information. Most frequently, the attacker suggests clicking a link or downloading software that contains malware or spyware which could compromise your personal and account information, potentially including financial and banking accounts.

Here are some tips to check if an email or text is legitimate

- Hover over the "from" address to see the full email address and make sure it is one you recognize and trust. Look for domain names that are slightly different or misspelled
- Be suspicious if the email asks for sensitive information such as passwords, bank account information, social security numbers, date of birth, or medical information in an email, chat session, or support call.

More ways to stay safe online

- Do not click on links or attachments in emails or text messages from senders that you do not recognize. If you hover over a link in an email, you will be able to see the location where the link will take you. Often, a link is suspect if it is long, confusing, contains typos, or mentions domains you do not recognize.
- Be especially wary of attachments like .zip or .pdf and particularly of executable file types (like those that end in .EXE). If you do not know the sender personally, you should never download or click these attachments.
- Do not provide sensitive personal information (like usernames and passwords) over email.
- Do not fall for messages that claim to be "urgent" or "time-sensitive". Often, scammers will try to scare you into sharing your personal information. Always take time to verify the identity of the requester and remember that reputable businesses will not ask you to provide sensitive information over email or over the phone.
- Pay attention to even seemingly harmless requests. A common ploy scammers use is emailing you a link to do something like change your account password. The link, in reality, will download malware or spyware.
- Do not open any document that you're not expecting to receive.
- If you can't tell if an email or text is legitimate, err on the side of caution and delete it. You can always call the business directly with any questions or concerns.