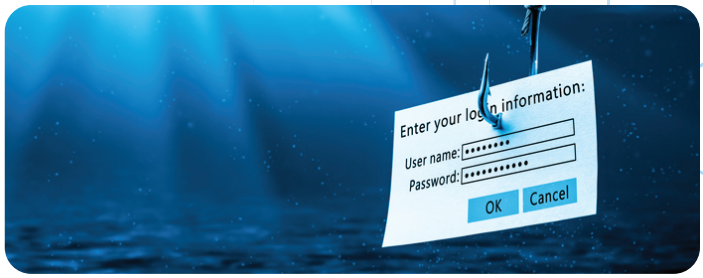
FRAUD AWARENESS

Email Phishing Scams



It's important to stay vigilant about email scams and phishing scams to protect yourself. Here are some common scams to be aware of:

Phishing Emails: These emails attempt to trick recipients into revealing sensitive information like passwords, credit card numbers, or social security numbers. They often impersonate legitimate organizations, such as banks or popular online services, and request personal information or ask users to click on malicious links.

Nigerian Prince Scam: This is a classic scam where scammers claim to be a wealthy individual or a government official from Nigeria or another country, promising a large sum of money in exchange for a small fee or personal information.

Lottery Scams: These scams inform recipients that they have won a large sum of money in a lottery, even though they may not have participated. The scammers then ask for personal information or request payment for processing fees or taxes before releasing the winnings.

Charity Scams: Scammers exploit people's generosity by posing as representatives of charitable organizations, especially during times of natural disasters or public crises. They request donations, but the money never goes to the intended cause.

Tech Support Scams: Scammers pose as technical support representatives from well-known companies, such as Microsoft and others, to contact individuals claiming that their computer has a virus or other technical issues. They aim to gain remote access to the victim's computer or extract money for fake services.

How to protect yourself from these scams:

- Be cautious about sharing personal information or clicking on links in unsolicited emails.
- Verify the authenticity of any email requesting sensitive information by contacting the organization directly through official channels. Do not call any number listed within the email. Open a new window in your browser and Google the official company / organization's phone number and email address.
- Keep your devices and software up to date with the latest security patches.
- Use strong, unique passwords for online accounts and enable two-factor authentication whenever possible.
- Be skeptical of offers that seem too good to be true or requests for immediate action.
- Regularly monitor your financial accounts for any suspicious activity.

Remember, education and awareness are key to avoiding scams. It is best to stay informed and to report any suspicious emails or incidents to the appropriate authorities.