PHISHING SCAMS

How to Recognize & Avoid Them

Phishing is a type of scam where criminals impersonate legitimate organizations in order to steal sensitive information. Scammers use fake emails, text messages or use online advertising to catch unsuspecting users in the scam.

EMAILS

- If the sender's address doesn't match the merchant, be careful.
- If it's not addressed directly to you, it's more than likely a mass email.
- If it's a generic greeting and not to you directly, it's probably a scam.
- If you find grammatical errors in the body of the email or the text and graphics are blurry, it's a sign that it's not legitimate.
- Don't click links or download attachments if it's unsolicited.

WEBSITES

- If the web address doesn't start with 'https', then it is not a secure site.
- You should be suspicious if the web address doesn't match the merchant's name or official site.
- If you find grammatical errors on the webpage, you should use caution.
- If graphics are low quality or links are dead, it's probably a dummy site.

TEXT MESSAGES

- Don't click on any links in text messages if you don't know the sender.
- If they are requesting personal information via text, it's a scam.
- If you're unsure if it's real, contact the company through the website or by a know/published phone number, not by text.
- Block phishing texts through your phone settings or wireless provider.

IF YOU THINK YOU'VE BEEN A VICTIM OF A PHISHING SCAM…

- Change all of your passwords to all of your accounts so they're not compromised.
- Contact the companies that were the object of the phishing to alert them to the scam.
- Use anti-virus software to scan your computer for existing viruses and malware.
- Watch your accounts to ensure no one is accessing them without your knowledge.
- Go to FTC.org and file a report with the Federal Trade Commission

1-800-938-8885

VIRGINIA SMP
Empowering Seniors To Prevent Healthcare Fraud

www.VirginiaSMP.com