TOWN OF Herndon

FROM THE IT HELP DESK: Don't get scammed!

Top Ten Scams and Phishing Attacks

1 Email Phishing

Be cautious of emails asking for personal information, login credentials, or financial details. Scammers often pose as legitimate organizations to deceive users.

2 Social Media Impersonation

Scammers create fake profiles impersonating known individuals, organizations, or celebrities to trick users into revealing sensitive information or sending money.

3 Fake Websites

Look out for websites with URLs that resemble well-known brands or organizations but have slight misspellings or variations. They may aim to steal your personal data.

4 Tech Support Scams

Scammers may contact you claiming to be from tech support, urging you to grant remote access to your computer and then steal sensitive information or install malware.

5 Phony Charities

Be cautious when donating to charities, especially during times of crisis. Verify the legitimacy of the organization before making contributions.

6 Lottery and Prize Scams

If you receive notifications of winning a lottery or prize you didn't enter, be cautious. Scammers often request payment or personal information to claim the prize.

7 Romance Scams

Online romance scammers build fake relationships to exploit emotions and solicit money or sensitive information from their targets.

8 Government Agency Impersonation

Scammers may pretend to be representatives from government agencies, threatening legal actions or fines to trick you into revealing personal details.

9 Job Offer Scams

Beware of job offers that require upfront payments or personal information. Legitimate employers do not ask for payment to secure a job.

10 Investment Scams

Be wary of unsolicited investment opportunities promising high returns with little or no risk. Do thorough research and consult trusted financial advisors before investing.

ALWAYS verify the authenticity of any communication or request for personal information.
Legitimate organizations typically won't ask for sensitive data through unsolicited emails, messages, or calls. When in doubt, directly contact the organization using official contact information to confirm the legitimacy of the request. Stay cautious and report any suspicious activities to relevant authorities.

Be on the Alert - Stay Cyber-Vigilant!