Beware of Phishing

From Public Safety Director Rosell
2018

Globally, cyber-attacks are increasing in frequency and sophistication at an exponential rate. In our ongoing effort to enhance the security our residents, we want to highlight a common cyber-attack that everyone should be aware of. **That attack is called phishing**.

"Phishing" is one of the most common forms of cyber-attacks. Phishing attacks can take many forms, but they all share a common goal – defrauding a person or company out of sensitive information (e.g. login credentials, credit card information, etc.) or goods and services. Phishers are now even going to the extent of impersonating Federal, State, and Local government entities in an effort to increase the efficacy of their attacks. By impersonating a government agency, or one of their representatives, the phisher is able to leverage the name and the authority associated with the name to lure in additional victims that would otherwise have ignored the phishing attempt.

We've outlined a few different types of phishing attacks to watch out for:

- **Deceptive Phishing**: In this type of attack, hackers impersonate a real company to obtain your login credentials. You may receive an e-mail asking you to verify your account details with a link that takes you to an imposter login screen that delivers your information directly to the attackers.
- **Spear Phishing**: Spear phishing is a more sophisticated phishing attack that includes customized information that makes the attacker seem like a legitimate source. They may use your name and phone number and refer to [COMPANY NAME] in the e-mail to trick you into thinking they have a connection to you, making you more likely to click a link or attachment that they provide.
- **Whaling**: Whaling is a popular ploy aimed at getting you to transfer money or send sensitive information to an attacker via email by impersonating a real company executive. Using a fake domain that appears similar to a legitimate business, they look like normal emails from a high-level official of the company, typically the CEO or CFO, and ask you for sensitive information (including usernames and passwords).
- **Shared Document Phishing**: You may receive an e-mail that appears to come from file-sharing sites like Dropbox or Google Drive alerting you that a document has been shared with you. The link provided in these e-mails will take you to a fake login page that mimics the real login page and will steal your account credentials.

The following industry best practices can help you avoid these phishing schemes, but also be sure to follow your organization's policies and procedures regarding email and cyber security:

- Do not click on links or attachments from senders that you do not recognize. Be especially wary of .zip or other compressed or executable file types.
- Do not provide sensitive personal information (like usernames and passwords) over email.
- Watch for email senders that use suspicious or misleading domain names and be familiar with how agencies release solicitation opportunities.
- Inspect URLs carefully to make sure they're legitimate and not imposter sites.
- Do not try to open any shared document that you're not expecting to receive.
- When replying to an email, ensure the TO: address in the reply email matches the email address of your intended recipient.