CLIENT RESOURCES

08/02/2021

IT Security Best Practices for HNW Families and Family Offices

Malicious Emails and Phishing

What Is Phishing and How Does It Work?

Phishing is a form of digital fraud in which a scammer, usually impersonating a trusted individual or company, influences a victim into giving money, disclosing sensitive information, or compromising an organization's IT infrastructure. The results can be devastating if not caught in time. For example, if criminals can gain access to an organization's IT backend, they can infect it with malicious programming, steal information, propagate more fraudulent emails, and/or cause other damage. The motives for launching a phishing scam vary, but criminals are usually after two things: money and/or information.

Phishing is part of a broader concept called "social engineering" or "pretexting" – the art of manipulating people with the use of publicly available (or otherwise discoverable) information to elicit extra layers of knowledge and trust in the communication. Not all scams are done by email, although many of them are email-based. Scams can be deployed via phone, social media messages, or other means. In the most common type of phishing, criminals send an email or text asking the victim to respond with information, click on a link, or download something.

How Can You Protect Yourself?

We recommend that all organizations regularly ensure they are following cybersecurity best practices, whether that means they have hired the right in-house talent or outsource this function to a trusted advisor to assist them. Regular and internal trainings and awareness campaigns are also key to keep

employees on alert to scammers' most recent techniques. It is also recommended that companies and organizations perform annual security assessments to check for risks and weaknesses. If you have questions about specifics around implementing best practices, we recommend you reach out to your IT professional team.

The Most Common Types of Phishing

Email Phishing: The Original

This scam often relies heavily on a "spray-and-pray" approach, where generic, templated emails are sent in bulk to many recipients at the same time. These emails usually impersonate a known or trusted company or individual. The goal is to trick someone into parting ways with personal information, such as login credentials or banking information. Attacks can also encourage an unsuspecting user to download a harmful file from a fake website, opening the door to a damaging malware infection.

All of this is made possible by what is known as "email spoofing," where email headers and subject lines are forged to make the email look as legitimate as possible. Phishing emails often appear to be from household names, such as Apple and Microsoft, due to their vast number of users and trusted reputation.

Spear Phishing: Time to Get Personal

Not all phishing scams are generic. "Spear phishing" fraudsters customize their emails to contain a specific individual's name, company, position, work phone number, and/or other information to trick the recipient into believing that they know or should know the sender. Spear phishing is especially popular on social media sites like LinkedIn, where attackers have a range of useful information.

Whaling: There's Always a Bigger Phish

In another scam involving the "bigger fish" of the organization, a "whaling attack" targets only an organization's top executives (whales) and ignores rank-and-file employees (smaller fish). Criminals will utilize research and social engineering techniques and include their findings in targeted whaling messages, so they can appear more credible and relevant. The more targeted and relevant, the more effective the communication is at getting through. The payoff can be higher when targeting leaders and executives at companies, because while there are fewer of them, they have access to more sensitive information.

BEC/CEO Fraud: The Art of Impersonation

In this increasingly common phishing scam, attackers pretend to be a CEO, CFO, or another executive of a company. After a successful whaling attack, criminals will hack into an executive's email account and spy on their activity until they have gathered enough information to effectively impersonate that executive. Next, they often send an email emphasizing urgency or high importance to someone else in the organization with a request to send money or sensitive information. While this is riskier for criminals to execute, it has proven to be very effective and has become a favorite scam among fraudsters. To counteract this type of scam, many companies have enacted strict policies of verbally confirming requests over the phone with a live person at a known phone number before executing requests.

How To Spot The Red Flags Of A Phish

1) Mismatched URLs

Often, the embedded URL in a phishing message will appear to be perfectly valid, but when hovering your mouse over the URL, the actual hyperlinked address may appear differently. This is an indicator that the link could be fraudulent.

2) Poor Spelling/Grammar

Large companies often have strict processes in place for reviewing company messages, especially when it comes to grammar, spelling, and legality. A message littered with mistakes may not be from a legitimate source.

3) Requesting Personal Info

No matter how legitimate or official an email looks, it is always a suspicious sign when it asks you for personal information. Banks and reputable companies will never ask you to send account or credit card numbers, as they should already know these details.

4) Others To Look Out For

- Special offers that sound too good to be true
- "Responses" from companies you've never contacted
- URLs containing a misleading domain name
- Unrealistic threats, like having your account deleted
- Emails that contain attachments/website links
- Messages that urge you to act quickly

We hope you find this information valuable. If you have any other questions, we urge you to contact your IT professional team.

This communication provided by Seiler LLP is general in nature and not intended to address any specific factual circumstances. Since this information is not intended to be a substitute for an individual/entity seeking professional expertise on specific factual situations, it should not be construed as creating a professional relationship between Seiler LLP and recipient on the subject matter contained in this communication. Although Seiler LLP has made every reasonable effort to ensure that the information provided is accurate, we make no warranties, expressed or implied, on the information provided.