This Week’s Tip: Data Entry Phishing Emails – Do Not Enter!

Data entry phishing emails remain one of the most effective ways for attackers to steal credentials and sensitive information. By using a malicious link to redirect victims to a fake login page, attackers can harvest sensitive information or credentials entered by the victim.

All too often, people give attackers exactly what they want. The good news: everyone can learn how to recognize and avoid these phishing attacks.

How Does Data-Entry Phishing Work?

An attacker will often pose as a trustworthy organization and send an email that urges you to click a malicious link. Clicking the link will direct you to a fraudulent website that requests specific information: account logins, banking details, personally identifiable information (PII), or other proprietary information. Attackers copy elements from legitimate websites to replicate the same look, feel and experience as the real page.

Once entered, the information is sent directly to the attacker who can then use it against you or your organization. Attackers can even redirect you to the legitimate website after the information is harvested. It is quite possible to fall victim to this attack and never notice.

What Can You Do?

There are several steps you can take to help you from becoming a victim to data-entry phishing, including:

- Always check the spelling of the URLs in email links before you click or enter sensitive information

- Watch out for URL redirects, where you are subtly sent to a different website with identical design

- If you receive an email from a source you know but seems suspicious, contact the sender directly with a known, verified phone number.

- If a website is asking you to submit personal information or log in, stop, and ask yourself these questions:

- Do I normally have to log in to this website to take this action?

- Is this website asking me to log in multiple times?

- Does this website really need this personal information from me?

- Is the website requesting details it does not normally ask for?

If you have any questions, please contact Information Security via Mark.Nagiel@SupremeLending.com. Thanks for participating in our team's efforts to keep our company data safe.