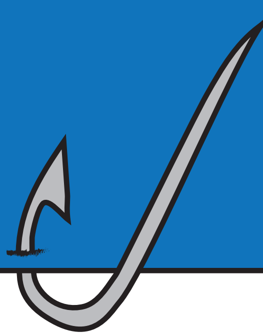
What is Phishing?



Phishing is a way for hackers to gain access to protected data, tricking people into giving away sensitive information such as bank credentials, social security numbers, passwords, and more....

...These emails look legitimate, and most people don't realize it's a scam until it's too late.

General Phishing: is sent in a blast for multiple people and acts like a boilerplate trying to attract someone to click and enter pertinent information.

Spear Phishing: is more direct, and a specific person (or specific group, such as executive, HR, or finance staff) is identified and targeted. The person of interest is sent an email from someone they trust asking for sensitive information.

What's the Point?:

When it comes to phishing, **the value isn't just in the money - it's in the information.** The social security numbers, passwords, and any other information acquired in a phishing attack can be sold to someone else. Phishing attacks can cause wide-ranging damage from ransomware related extortion and data-loss, to the theft of information which can then be used to give someone a new identity or to open up lines of credit in your name.

Strong Technology

www.strongtc.com

How to Identify Attacks

Recognizing phishing attacks can be difficult because they are socially engineered to look like they are coming from a trusted source...

... but, there are a number of warning signs that can give them away if you know what you're looking for.

What to look for:

- The email will likely be **asking for personal information.** It might say something along the lines of "your password has expired, update it here by clicking this link" (leading you to a spoofed website).
- **Grammar errors-** This could be as subtle as one misspelled word or something more noticeable like awkward sentence structures.
- **Branding that's just slightly off-** Many phishing emails will "copy" the branding and banners of well-known companies to make their emails more convincing. However these will often be one or two shades off, use different fonts, or misspell names, dates, info, etc.
- **The hyperlink goes somewhere else-** Anyone can change the hyperlink in an email to send you to a different website than it claims. Before you click, hover over the link to check where it's really taking you.
- **Beware of anything before the forward slash-** Adding periods or dashes before the forward slash tricks people into clicking on links because it looks like the right URL at first glance. For example http://payapl.com-stz.info/ isn't going to paypal.com

Best Practices

For your business

When it comes to phishing, the user is both your strongest defense, and your weakest link. Hardware and software can only go so far to protect your systems, but if users are knowledgeable, phishing can be more preventable.

Avoid Phishing scams by:

Keeping phishing training up to date- Have your employees take phishing training annually or biannually to familiarize them with threats. Educated users are harder to trick.

Don’t click on any suspicious emails- If you’re not expecting an email don’t click. Instead, check with the individual it came from to confirm the request before sending personal information.

Take the time to look at the details- Phishing scams are so detrimental because missing one simple spelling error or forgetting to check a link can lead to trouble. Most scams come from places you would normally trust, causing you to fill in the information without thinking about it. This is how cybercriminals prey on your trust.

Keep your information compartmentalized- If your employees don’t need information to complete their job, don’t give them access to it. Running your business on a less privileged basis will help minimize the chances of leaking confidential information.