HACKER COMBAT COMMUNITY

PHISHING STOPS HERE

Learn How To Identify and Avoid Phishing Scams

- The average financial cost of a data breach is $3.86 Million (IBM)
- Phishing accounts for 90% of data breaches
- Phishing attempts have grown 65% in the last year
- Around 1.5m new phishing sites are created each month (Webroot)
- 30% of phishing messages get opened by targeted users (Verizon)

Learn what phishing is, the latest cyber attacks using phishing tactics, and how to prevent phishing attacks.

What is a Phishing attack?

Phishing is a form of online identity theft that aims to fraudulently obtain personal information by sending spoofed emails that look like they come from trusted sources, such as banks or legitimate companies.

By masquerading as a reputable source with an enticing request, an attacker lures in the victim in order to trick them, similarly to how a fisherman uses bait to catch a fish.

The most common examples of phishing are used to support other malicious actions, such as man-in-the-middle and cross-site scripting attacks. These attacks typically occur via email or instant message, and can be broken down into a few general categories. It's useful to become familiar with a few of these different vectors of phishing attacks in order to spot them in the wild.

Phishing scams continue to proliferate at alarming rates and are becoming more and more difficult to detect. It's important for you to understand how to recognize a phishing attempt and what you can do to protect yourself.

Detecting and Defending Against Phishing Attacks

One of the most persistent security challenges is phishing. This is true for both organizations and individuals.

Whether gaining access to credit card information, security passwords, or any other sensitive information, hackers can use different techniques, such as social engineering, emails, phone calls, and other forms of communication, to steal data. This opens up businesses as worthwhile targets, since they have valuable data on hand.

In order to help businesses avoid losing data from phishing attacks, we've gathered information from different security experts to share their views on this and the best practices that companies can do in order to protect themselves.

What is the single biggest mistake a company can do that makes them vulnerable to phishing attacks?

- When the company does not invest in the right tools and they do not provide proper training to their people about their role in information security.
- Browsing the internet carelessly.
- Not having proper policies that outline how to react to suspicious emails.
- When organizations are run in an authoritarian style where employees are trained to simply follow instructions, which leads them to easily giving up information.
- The same can be said for organizations that have a culture where asking for help is frowned upon.
- Not using a multi-layered approach to detect, analyze, and stop phishing attacks.
- Spear phishing is becoming more and more popular to target specific employees, so there is a bigger need to train employees about protecting their data.

While there are any different specific things that the security experts mention, there is one in common that can be picked out from these: Phishing attacks are geared toward people. Hackers use social engineering in order to get the information they need from company employees.

This strengthens the fact that training employees on phishing defense is crucial to stopping these attacks.It also highlights the importance of crafting proper policies and protocols in the event of such attacks.

What are the common ways that cyber criminals attack?

- Sending a link through email that opens a malicious website.
- Placing a trojan in the target's computer through an email attachment.
- Creating a spoofed email to look as reputable as possible and tricking the receiver.
- Impersonating a vendor or IT department and calling via phone.
- A technique where content with malicious intent is injected into the company's website to obtain passwords.
- Hackers positioning themselves in the middle of the company and their customers to capture any and all information transmitted between them.
- DNS-based phishing attack that forces people into a malicious website when they try to visit the target website.

How Can We Defend Against Phishing Attacks?

- Use an SSL certificate on your website to protect all information transmitted between the web server and the visitor's browser.
- Provide proper and regular training to employees about phishing, how to identify it, and what to do when they suspect an attack.
- Ensure that all security tools, protocols, and controls are up to date. Also, take note of new developments in the IT industry about tools and new types of attacks, to be able to adapt the company's defenses.
- When a payment page is needed for your website, make sure to use a securely hosted page. This is the best practice in order to secure credit card information being transmitted over the internet.

How Can We Defend Against Phishing Attacks?

- Create a filter that can detect the most common types of spam and phishing attacks. This should be also able to identify attachments and filter malicious ones.
- Use an antivirus solution for each endpoint device, as well as the entire network.
- Encrypt the sensitive data of the company so they are difficult to open even when stolen.
- Use a web filter in order to block malicious websites from even opening on your network.
- Disable HTML email feature within the organization, which will reduce the risks of phishing attacks.
- Make sure to require proper encryption for all employees who telecommute or work remotely.

Remember, all it takes is for one employee to take the bait, and the organization can fall into chaos.

The IT department can set up several layers of defense against such attacks as mentioned earlier, but each employee needs to participate in ensuring that all data is protected.

Do not open suspicious emails, avoid browsing malicious websites, and never open an attachment from an email that you do not know the sender. These are just a few simple best practices that can be adopted by each employee in order to deter phishing attacks.