VareseNews

Why you will be targeted by phishing attacks

Pubblicato: Mercoledì 9 Dicembre 2020

If you go online for most any reason, it's safe to say that you can be targeted by phishing attacks at one time or another (if it hasn't already happened to you, that's good news!).

Phishing is an easy method for criminal hackers to gain unauthorized access to valuable data. Individuals who do not follow basic Internet safety protocols, such as by always using a virtual private network or VPN when connecting to a public Wi-Fi network are particularly vulnerable.

Startling statistics about phishing abound. For example 98% of malware is known to come by email, and 48% of emails that have malicious attachments are Microsoft Office files, according to Phishing Box.

What Are Phishing Attacks?

Criminals will contact you by email or text messages, in an attempt to get you to reveal some details about yourself. The object is to get your password or trick you into divulging your Social Security number or the routing details for your bank.

In a phishing expedition, you might receive an email that looks legitimate, but it's not really from your streaming video service or bank asking you to log in. Instead, you are taken to a counterfeit site and once you type in your secret password, the hacker has your information.

Sometimes a scammer will try to get you to download a file in an email attachment. You should never accept or open a file from a stranger. Once clicked, it can infect your computer with a virus that then steals or wipes out your important data.

Who Is Vulnerable to Phishing?

Anyone who is online is subject to a phishing attack. However, hackers using this technique will be especially attracted to certain types of people. For example, criminals can profit by attacking:

* Political Figures and Their Support Team: A hacker, whether from an opposing political party or a malicious actor from another country could use phishing to sow chaos or influence the results of an election.

If they trick someone into clicking on a link that sends them to a malware-riddled site, the campaign's information could become compromised.

* Famous Individuals: Imagine a famous person tricked into thinking he or she is communicating with a legitimate individual and then gives out personal information bit by bit.

The hacker will use these details to try to figure out a password. At this point, it's trivial to break into a bank account or email. The hacker could also use the data breech to impersonate the celebrity on social media, putting out bogus Facebook posts and tweets that get the famous person into trouble.

* Wealthy People: Since hackers often use phishing as a means to steal money, they will want to pry their way into the finances of individuals of great wealth. A rich person who thinks his success comes from being smarter than others may think he is too clever to be fooled by hackers.

Then after a phishing attack, the wealthy victim learns a lesson to rely on the wisdom of security experts to safeguard computers, tablets and smartphones.

* Employees of Companies Holding Valuable Data: Sometimes what's of interest to hackers will not necessarily be money from people's bank accounts, but private information stored on an enterprise's data servers.

First, a hacker tricks a lower level employee to take the bait (clicking a link to a hacked site or downloading a malicious file, for example. This launches an attack on the company's computer network.

If the hacker deployed ransomware, it will lock up the company's computers, holding the data hostage. The victims are instructed to send a ransom via digital currency in exchange for the criminals freeing up the data.

Problems for People Targeted by Phishing

To motivate yourself to take computer security more seriously, keep in mind that victims of phishing attacks can wind up having to sort out a tangled mass of problems.

They may have to apologize to everyone in their contacts list because after a phishing attack placed malware on their smartphone, it sent them all a message with a virus-carrying attachment.

Your bank account can be emptied out when a phishing attack yields your bank login. If the hacker obtains your email password, he might use it to reset passwords on other accounts too, locking you out of social media. A criminal might have targeted you because he thinks you have work secrets on your laptop.

What's more, if your company is involved, you run the risk of being fired because you didn't follow security protocols, leaving sensitive information on a vulnerable device that criminals accessed after their phishing expedition.

Protecting Yourself Against Phishing

It's best to keep your computer and portable devices updated. When the manufacturer or software developer tells you about an update (especially a security update), you'll want to download it.

If you feel comfortable to let your computer or phone take care of this process automatically, you won't need to worry about missing future updates. But if you'd rather double-check that a operating system update won't affect your important apps, do so as soon as possible.

Postponing a security update that addresses known problems isn't a good idea. It would mean that those security holes will continue to leave your device open to hackers until you finally allow the update.

It's also prudent to maintain backups of all of your important data, in case a phishing attack does happen and you need to restore your data (this would allow you to refuse to make a ransomware payment to a criminal, for example.)

For additional peace of mind, the Federal Trade Commission recommends that you use multi-factor authentication to safeguard your accounts. This involves using at least two other credentials when logging in. You'll receive a temporary code to type in along with your name and password for online

banking. Or, you have to scan your fingerprint with your smartphone when signing in.

Be Prepared!

It only takes a moment to protect yourself from phishing attacks. A small amount of effort to protect your online accounts now will keep you from enduring hours of sorting out the mess that hackers leave in their wake after breaking in.

Redazione VareseNews
redazione@varesenews.it