tigunia Phishing Attacks

How to Recognize Phishing and Keep Business Data Safe

Cybercrime is on the rise, and hackers are using any opportunity to take advantage of an unknowing victim to gain access to personal information for financial gain. The new 'work from anywhere world' makes everyone at risk to cyber attacks, especially because threats are harder to track over home networks. The blurred lines between home and work create security nightmares if safety protocols are ignored, or don't exist.

One commonly used tactic is phishing. Phishing messages are crafted to deliver a sense of urgency or fear with the end goal of capturing a person's sensitive data. If your employees fall prey to phishing scams while working from home, it can affect your company network by transferring malware and viruses over internet connections. One phishing email has the power to cause downtime for your entire business. Unfortunately the scams are getting more sophisticated on a daily basis, thus harder to detect.

Common Types of Phishing Attacks

Spear Phishing

Attackers pass themselves off as someone the target knows well or an organization that they're familiar with to gain access to compromising information (e.g., credentials or financial information), which is used to exploit the victim.

Whaling

Whaling is a form of spear phishing with a focus on a high-value target, typically executives or high-level employees, usually to gain access to company platforms or financial information.

Mass Campaigns

Mass phishing campaigns cast a wider net. Emails are sent to the masses from a knock-off corporate entity insisting a password needs to be updated or credit card information is outdated.

Ambulance Chasing Phishing

Attackers can use ongoing crises to drive urgency for victims to take action that will lead to compromising data or information. For example, bad actors used the COVID-19 crisis to solicit donations, embedding phishing attacks in the emails.

Pretexting

Pretexting involves an attacker doing something via a non-email channel (e.g., voicemail) to set an expectation that they'll be sending something seemingly legitimate in the near future only to send an email that contains malicious links.

What to Do If You Receive a Phishing Email

First, to help identify it as a phishing email, check to see if the signed-by field was generated by a DomainKeys Identified Mail (DKIM) or a service. DKIM is a good first step in email authentication and is a technical solution to prove that an email is not fake. For example, if you received an email from name@technology.com, you would see a DKIM in the signature that looks like this: technology-com.20150623.gappssmtp.com. This is how all emails through a domain are processed.

Emails shared through a service (e.g., Drive, Calendar, Dropbox, Box, etc.) do not have a DKIM. Instead, you would see the signature of the provided service (i.e., signed-by dropbox.com). If you receive a file, and it is not signed by google.com, gmail.com, dropbox.com, it is likely phishing - delete it immediately. It's important to remain vigilant and proceed with caution in these circumstances.

Get additional training and insight today by contacting a Tigunia representative.