Protecting your business from phishing and malware attacks

As a business owner you know that IT is critical in helping you run your business successfully. No matter what your business, it simply cannot run without IT being involved in some form. Whether you serve customers online, sell your products/services using the internet marketplace/e-commerce sites or simply have a website while the rest of your business is offline, IT has a role to play. This whitepaper discusses major threats to your business from the IT perspective–phishing and malware attacks, for example– and explains how you can safeguard your business against them.

Phishing

In phishing attacks, cybercriminals generally send a web link that is disguised to look genuine, and prompt the receiver to share information that will then be misused. For example, an email may be sent to you that looks as though it came from your bank or the IRS announcing a tax refund that your business is eligible to receive. You may be asked to log into your bank account or a fake IRS site and enter your bank details to receive the refund or download a receipt. The cybercriminals will have access to any details you share and later use it to clear out your bank account.

Phishing links may also lead to clone websites. Clone websites, as the name suggests, are websites that look strikingly similar to original websites, but are obviously not the same and are controlled by cybercriminals and used to steal data from unsuspecting victims. Here are a few tips to help you identify clone websites and steer clear of them.

If you receive an email with a link to a familiar website asking you to log into the site or enter your personal information, cross check the URL. Check the spelling and domain, for example, www.amazon.com. is the right URL, whereas a clone website may have an URL that looks similar

but is not the same. An example would be www.amaazon.com or www.amazon-offer.com Another thing you can do is, always type the URL you intend to visit. For example, if you are being asked to log into your bank account, type your bank's website address instead of clicking on the link they provided to you in the email.

Sometimes, phishing attacks can be manual as well, meaning, instead of asking you to enter your personal information in a website or a form, the cybercriminal may pose as someone you know and send you an email from an email address that looks authentic and try to get money or personal information from you. Such attacks usually happen if your network or that of your recipient's has been compromised in a hacking attack, whereby the cybercriminal has some information that they can use to make their messaging sound genuine.

Ransomware and other malware attacks

Phishing is a way to get access to personal information and probably even to your IT network by stealing access credentials, but that's not the only way. Cybercriminals also deploy various malware such as viruses, worms and trojan horses to attack IT networks. These malware usually gain entry into the system disguised as genuine email attachments, links to file downloads, etc. and then corrupt the data. In the case of ransomware, as the name suggests, the malware attack goes beyond data corruption and the cybercriminals hold the data hostage and demand a ransom from the business for restoring data access.

While malware and phishing attacks have evolved over time and are constantly becoming more and more sophisticated, there are ways to protect your data from them. Here are a few best practices to follow that can help safeguard your business.

Install a strong firewall
A firewall can help prevent unauthorized access to your network by monitoring access attempts and allowing or rejecting them. Firewalls are flexible in the sense that you can choose how stringent or lenient you want it to be in terms of limiting access. There are different kinds of firewalls, each serving a particular purpose and offering different protection levels. Firewalls basically work to block unauthorized traffic to your network based on various factors including IP address, location and any other custom parameters that you may choose. Without a firewall, your network is essentially open, exposed to any one on the web, which puts you at serious risk.

Invest in antivirus software
Antivirus software programs identify viruses and other malicious attachments that cybercriminals may use to gain entry into your system or network. Make sure you invest in a good antivirus software and update it regularly so it can protect you against newer versions of malware that crop up with time.

Train your staff

Train your staff to identify and steer clear of phishing emails, links and messages. Educate them on password hygiene, safe web surfing, and basic IT best practices even when using their own devices. You can provide training in-person and conduct mock drills and IT workshops. Also, consider sending regular emails on these topics so your staff remains alert. Security training isn't a one-off project. Also update your staff on any new vulnerabilities discovered and if there are any security updates or patches released for them in the market, then be sure to apply them immediately.

While all of the actions discussed above are important and you can't afford to ignore them, it can be difficult to keep up with them and perform them consistently...especially when you have a business to run and are caught up in day-to-day operations. It makes sense in such a scenario to bring an experienced Managed Services Provider (MSP) on board who can help you with data security, training and general up-keep and maintenance of your IT infrastructure.

For more information contact:
Michael Mendoza
877-343-1409
michael@aristocyber.com