Recognizing the Many Faces of Phishing:

A Guide for Small-Medium Sized Businesses

axishield

What is Phishing?

At its core, phishing is a cybercrime that uses deception to steal sensitive information or install malware on your systems. While the methods may vary, all phishing attacks share a common goal: **exploiting human behavior to breach your defenses.**

In today's digital landscape, cybersecurity is no longer just a concern for large corporations. **Small and medium-sized businesses (SMBs) are increasingly becoming targets for cybercriminals**, with phishing attacks being one of the most common threats. As an SMB owner or manager, understanding the various types of phishing can be your first line of defense against these sophisticated scams.

axishield

How to Protect Your SMB from Phishing Attacks

While the variety of phishing attacks may seem overwhelming, there are steps you can take to protect your business:

Employee Training: Regular cybersecurity awareness training is crucial. Teach your team to recognize the signs of phishing across all platforms.

Keep Software Updated: Ensure all systems and software are regularly updated to patch known vulnerabilities.

Create a Security-First Culture: Encourage employees to report suspicious activities without fear of reprimand.

Engage with a Cybersecurity Partner: Partnering with a Managed Service Provider offering cybersecurity solutions provides your business the protection it needs.

5 Types of Phishing to Watch For

axishield

1

SPEAR PHISHING: THE PERSONALIZED THREAT

Imagine receiving an email that seems to know you personally – that is spear phishing. Unlike generic phishing attempts, spear phishing is tailored to specific individuals or organizations. Cybercriminals research their targets using social media and company websites to craft convincing, personalized messages. These emails often contain malicious links that, when clicked, can infect your computer with malware.

HOW TO PROTECT YOURSELF:

Encourage employees to verify unexpected requests, even if they seem to come from known contacts. Implement a policy of confirming sensitive requests through a different communication channel.

axishield

2

VISHING: THE VOICE OF DECEPTION

Vishing, or voice phishing, takes the scam off the screen and onto your phone. Fraudsters use spoofed caller IDs to appear as trusted sources, often posing as bank employees or government officials. They create a sense of urgency to pressure victims into divulging sensitive information like login details or PINs.

HOW TO PROTECT YOURSELF:

Train your staff never to provide sensitive information over the phone, especially when they didn't initiate the call. Encourage them to hang up and call the organization directly using a verified number.

axishield

3

WHALING: FISHING FOR THE BIG FISH

Whaling targets the big fish in your company – senior executives and high-level employees. These attacks are highly sophisticated, often using corporate language and personalized information to appear legitimate. The potential payoff for criminals is higher, so they invest more time and effort into crafting these deceptive messages.

HOW TO PROTECT YOURSELF:

Implement extra security measures for high-level accounts, such as multi-factor authentication. Provide specialized training for executives on recognizing these targeted attacks.

4

SMISHING: SMS PHISHING

As our reliance on mobile devices grows, so does the threat of smishing. This technique uses SMS messages to trick individuals into revealing personal information or clicking on malicious links. These texts often create a false sense of urgency, prompting immediate action from the recipient.

HOW TO PROTECT YOURSELF:

Advise employees to be wary of unsolicited text messages, especially those requesting immediate action. Encourage them to verify the sender through official channels before responding or clicking any links.

axishield

5

CLONE PHISHING: THE FAMILIAR FACE

Clone phishing is particularly sneaky. Attackers take a legitimate, previously delivered email and create an almost identical clone – but with malicious content. The email appears to come from the original sender, often claiming to be an update or resend of the previous message.

HOW TO PROTECT YOURSELF:

Implement email authentication protocols like DMARC to prevent email spoofing. Teach employees to be cautious of unexpected "resent" emails, even from known senders.

axishield

Protect Your Business with AxiShield

AxiShield is a robust and holistic cybersecurity solution, designed to not only protect your company but also educate your employees on avoiding potential threats like phishing. Our cybersecurity solution is customizable to the needs of small and medium-sized businesses (SMBs), featuring automated reporting, dashboards, and streamlined management which allows you to continuously recognize the value of your investment.

axishield

Schedule a meeting today to protect your business.

Visit www.axiatp.com/cybersecurity for more information or contact us for a complimentary consultation.

axishield