POSTED BY MARK MEISSNER ON 31 AUG, 2021 IN SOFTWARE AND SMALL BUSINESS AND ECOMMERCE AND BREACHES AND GUIDANCE AND PATCHING AND PASSWORDS AND FIREWALLS AND MALWARE AND HACKERS AND PHISHING AND AWARENESS AND SMALL MERCHANT RESOURCES AND SMB SERIES AND BAU AND MULTI-FACTOR AUTHENTICATION AND COVID-19 AND BACK TO BASICS

As small and medium businesses begin to re-open following the pandemic, it's important to do so securely in order to protect customer's payment card data. Too often, data breaches happen as a result of vulnerabilities that are entirely preventable. The PCI Security Standards Council (PCI SSC) has developed a set of payment protection resources for small businesses. In this 8-part back-to-basics series, we highlight payment security basics for protecting against payment data theft. Today's blog focuses on thinking before you click.

Hackers use phishing and other social engineering methods to target organizations with legitimate-looking emails and social media messages. These trick users into providing confidential data, such as credit card numbers, social security numbers, account numbers, or passwords.

These attacks have been around for a while and are at the heart of many of today's most serious cyber-attacks and can put your business and your customers at risk. It is important to have your guard up when opening emails and engaging in social media. Everyone needs to be aware of how to best protect against phishing and social engineering attacks.

There are many ways to defend against this type of attack including the following best practices:

Reduce unwanted email traffic:

- Install and maintain basic security protections, including firewalls, anti-malware software and email filters to prevent known malicious IP addresses or domains for example.

Train employees and users on email and browser security best practices, including these key tips:

- Resist the urge to click links in a suspicious email; visit websites directly.
- Be cautious of email attachments from unknown sources. Also, many viruses can fake the return address, so even if it looks like it's from someone you know, be wary about opening any attachments.
- Only install approved applications.
- Be sure you're at the right website when downloading software or upgrades. Even when using a trusted site, double check the URL before downloading to make sure you haven't been directed to a different site.
- Recognize the signs that your computer is affected and contact IT.

Update Regularly:

- Use basic security tools that block malicious intruders and alert you to suspicious activity, including firewalls, anti-virus, malware and spyware detection software.
- Regularly check that web browsers and security software have the latest security patches and updates.

Separate Personal-Use Devices from Work Devices:

- Keep computers used for social media sites, email and general internet browsing separate from computers used for processing financial transactions.

Practice good password hygiene:

- Change the passwords on computers and point-of-sale systems (including operating systems, security software, payment software, servers, modems, and routers) from the default ones the product came with to something personal to you but that is difficult to guess - such as combining upper case letters, numbers and special characters, or using a passphrase.
- Update system passwords regularly, and especially after outside contractors do hardware, software or point-of-sale system installations or upgrades.
- Educate employees and users on choosing strong passwords and changing them frequently.

Use two-factor authentication:

- Many of these attacks rely on getting a password one way or another. Requiring another form of ID, such as security tokens, will make it harder for hackers to falsify an account.

Still working from home? Take this 45-minute training to ensure your work set-up is secure: New Training: Work from Home Security Awareness.

View the Back-to-Basics Series

## Mark Meissner

As SVP, Education & Engagement Officer, Mr. Meissner works to develop education and engagement strategies that promote the PCI Security Standards and the priority initiatives of the PCI SSC globally and with a wide range of stakeholders.