Protect your online business against cyberattacks

As a small and medium business, you are a target for cybercriminals. Using the internet, these data thieves attack and steal your customers' payment (debit and credit) card data to commit fraud. This data is especially at risk when it travels to your merchant bank, and when it's kept or stored on your computers and devices. Using encryption and tokenization technologies to devalue the data so it can't be used fraudulently if stolen is the best way to protect your business. **On top of this, businesses must stay vigilant to protect their computers and systems.**

of cyberattacks worldwide were against businesses with less than 250 workers

(Source: 2016 Internet Security Threat Report, Symantec)

HERE ARE 3 TIPS ONLINE BUSINESSES CAN TAKE NOW TO BOOST SECURITY:

63% of confirmed breaches involved weak, default or stolen passwords.

(Source: 2016 Verizon DBIR)

1 CHANGE YOUR PASSWORDS AND MAKE THEM STRONG!

- Use a passphrase, which is just a phrase or sentence, instead of a single word. Use numbers, symbols/ special characters and letters including upper and lower case. For example, "1l0v3B!GD@nut$".
- If the password you're using is "Password1" – change it! It's one of the most common passwords used, and criminals know it. Just like you lock the doors before you leave – lock this door too.
- Educate your staff – take a break together and discuss changing passwords to passphrases.

PCI Resources to Help You: It's Time to Change Your Password; Guide to Safe Payments; PCI DSS requirement 2.1, 8.2.3 – 8.2.6, 8.4

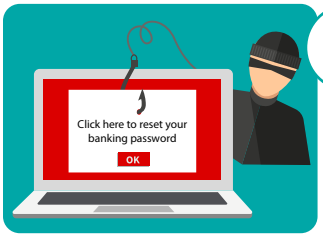
Software vulnerabilities are the main reason for breaches occurring.

(Source: 2016 Verizon DBIR)

2 INSTALL THE UPDATES KNOWN AS "PATCHES" THAT YOUR PAYMENT SERVICE PROVIDER SENDS YOU FOR YOUR PAYMENT SYSTEMS

- Just like you install updates on your phone – install patches on your payment systems to ensure you're protected from the bad guys trying to find a way to break in. Patches and updates fix problems found in the system as well as provide new features.
- Those problems are often the main reason a system gets breached. Install updates from your payment service provider to make sure you've plugged the holes that criminals can use to get into your systems. Keep them out – install the patches.
- Likewise, make sure your e-commerce hosting provider (they host your web site) periodically installs patches on the e-commerce systems and/or web applications they host for you – ask them!

PCI Resources to Help You: Guide to Safe Payments; PCI DSS requirement 6.2



Beware of "phishing" attacks!

3 KEEP BUSINESS INFORMATION PRIVATE!

- Just like you wouldn't tell a customer the code for your front door or give a random stranger your bank details, keep your passwords, user IDs, and other important details for your payment systems private.
- "Phishing" attacks are on the rise. These attacks happen when a criminal calls you up or sends an email asking about the systems you use, what your passwords are, etc. They may even pretend to be from your payment service provider, bank, or another business partner – always separately confirm an unexpected call or email with that entity claiming to make the call before proceeding. The person may want to use the information to get into your systems and steal data. Make sure your employees know to keep that information private. The risk to your business could be devastating.
- Another common "phishing" trick criminals use is to send you an email that asks you to click on a link or open an attachment. Once you do, that causes malware to infect your systems. Even if the email says it comes from someone you know – confirm with the sender first. If the sender is unknown to you, delete it.

PCI Resources to Help You: Guide to Safe Payments; Defending Against Phishing & Social Engineering Attacks

PCI Security Standards Council ®