HOLIDAY SEASON SECURITY TIPS FOR SMALL MERCHANTS

With more individuals shopping online these days, and with more businesses offering their goods and services via an e-commerce platform, it's important merchants understand what steps they can take to protect their business and customer data from cyber criminals.

TAKE-ACTION TIPS

LOCK DOWN YOUR LOGIN

Fortify your payment terminals, accounts, and e-commerce platforms with long and unique passphrases for all accounts and use multi-factor authentication (MFA) wherever possible. MFA will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device.

.

DON'T HESITATE TO UPDATE

Keep the software on all Internet-connected devices up to date. All critical software, including computer and mobile operating systems, security software, e-commerce software, and other frequently used programs and apps, should be running the most current versions. Turn on automatic updates in the security settings.

BE OPEN FOR BUSINESS AND CLOSED TO CYBER CRIMINALS

As consumers increasingly shop from the safety and security of their homes, criminals will take advantage of this situation by not only targeting attacks on consumers, but on merchants as well. As you build your online e-commerce capabilities, build security into that strategy.

THINK BEFORE YOU CLICK

Criminals will try to trick you by pretending to be your bank, payment processor, trusted business partner, etc. If you receive an email encouraging you to take action, do not be so quick to click on the link. Instead, call the company directly or go to their website (not using the contact information in the email itself).

HOLIDAY SEASON SECURITY TIPS FOR SMALL MERCHANTS

TAKE-ACTION TIPS

LIMIT ACCESS

Do an audit of who has administrative or privileged access to your e-commerce site and payment data. Restrict that access to only those who need it to do their jobs.

BACK IT UP

Protect your sensitive information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware or other cyber threats, you will be able to restore the data from a backup. Use the 3-2-1 rule as a guide to backing up your data. The rule is: keep at least three (3) copies of your data, and store two (2) backup copies on different storage media, with one (1) of them located offsite

ENCRYPT YOUR PAYMENT DATA

Check with your vendors to see if they encrypt payment data while it is being stored and transmitted so that you can hide sensitive data from criminals.

SEEK HELP

Criminals are always targeting consumers and merchants, but increase their efforts during busy online shopping periods. Talk to your payment vendors and to your information security professionals in your community so you can fortify your defenses ahead of the season.

ADDITIONAL RESOURCES

- **Cybersecurity & Infrastructure Security Agency:** Cybersecurity Tips
  https://www.us-cert.gov/ncas/tips
- **Federal Trade Commission:** Cybersecurity Basics
  https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/basics
- **PCI Security Standards Council**: Shopping Safely Online
  https://www.pcisecuritystandards.org/document_library?category=educational_resources&document=pcissc_covid
- **Adobe & NCSA Security Awareness Video:** Phishing and Ransomware:
  https://youtu.be/D_yAYhjNE-0