

HOLIDAY SEASON SECURITY TIPS FOR SMALL MERCHANTS

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



BE OPEN FOR BUSINESS AND CLOSED TO CYBER CRIMINALS

Criminals will take advantage of the busy holiday season 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 to keep your business running smoothly throughout the holidays and all year long!



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.



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 an immediate 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).



TIPS FOR SAFE ONLINE HOLIDAY SHOPPING



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 copies and storing them 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: 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>

