WELLS FARGO Wealth & Investment Management

Helping protect your small business from the latest cyber threats

As a small business owner, would you be able to maintain business operations if your systems and data were to become unavailable due to a cyberattack? Do you have a business continuity and recovery plan, and is it up to date? If you don't have a resiliency plan or are feeling dreadfully unprepared, you're not alone. According to a 2021 Small Business Administration (SBA) survey, 88% of small business owners felt vulnerable to a cyberattack.[1]

Many small businesses have limited time and resources to devote to cybersecurity, cannot afford to hire or outsource information-technology solutions, or they don't know where to begin. Here are some cybersecurity best practices to help get you started.

By the numbers

93%

of businesses that lost their data for 10 or more days filed for bankruptcy within one year and 50% filed for bankruptcy immediately[2]

$9.6 billion

of cybercrime losses were reported to the FBI in 2021. That's a staggering increase of 64% from the prior year loss of $4.2 billion and 393% since 2017 when the total loss was $1.4 billion[3]

Sources:
1 - Protect Your Small Business from Cybersecurity Attacks (sba.gov) (2021)
2 – https://www.weforum.org/reports/global-risks-report-2022/in-full (2022)
3 - https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (2021)

Investment and Insurance Products: Not FDIC Insured / No Bank Guarantee / May Lose Value

Helping protect your systems and processes

Establish a business continuity plan (BCP)

Establish a business continuity plan (BCP) to help minimize any operational and financial losses. Be prepared and have a plan in the event your business becomes the victim of a cyberattack. Know what that plan is, and test it regularly to help ensure it is up-to-date and meets the needs of the business. As the adage goes, failure to plan is a plan for failure.

The Federal Communications Commission (FCC) offers a free online resource called Cyberplanner to help small businesses create customized cybersecurity plans to help protect their business.

Update your software and antivirus

Ensure all endpoint devices on your network are running the latest firmware and software and your network is protected by a firewall. Make sure your Wi-Fi network is password-protected and uses encryption. Enable your systems to install software updates automatically to help protect against viruses, malware, spyware, network threats, and zero-day exploits.

Require strong passwords

Use strong passwords to help protect your accounts/systems and change them on a regular basis. Avoid using easy-to-guess passwords such as pet names, birthdays, 12345, etc., and do not use the same username and password across multiple accounts/systems.

If your username and password become compromised, your entire network can be put at risk. Consider using a passphrase or alphanumeric password that contains a combination of uppercase, lowercase, and special characters as well as a password manager app to track all your usernames and passwords.

Enable multifactor authentication (MFA, 2FA) for access

MFA/2FA requires something you know (your password) and something you have (such as a unique code sent to your email or mobile device.) Authenticator apps like Microsoft Authenticator and Google Authenticator are becoming increasingly more popular — after you enter your password, you receive a request on your mobile device to approve the account log in. Using MFA/2FA will significantly decrease the likelihood of you getting hacked.

Manage cyber supply-chain risk

Businesses need to adopt a variety of practices to help manage their supply-chain risk. Set minimum security requirements for your suppliers, and develop defense with “assume breach” in mind. This means a business approaches its cybersecurity anticipating that there is already a compromise.

The National Institute of Standards and Technology (NIST) has an established framework for cybersecurity supply-chain risk management.

Backup, backup, backup!

Your business should have multiple data backups — an online backup (i.e., cloud-based storage solution) preferably stored on a separate network isolated from your primary business operations and a secondary physical backup stored at a secure offsite location.

Identify your computer network ecosystem and critical data

What are your "normal" operating processes and system activity? Establish a baseline so you can monitor against it. Monitor all accounts, systems, and network activity for unauthorized access, abnormal processes, and unusual or inconsistent activity. Monitoring should include potential insider threats as well.

Business email compromise (BEC)

Be wary of business email compromise (BEC) scams, which can include a fraudulent request for payment to a vendor or supplier. Also known as imposter fraud or CEO fraud, BEC is a type of cyber scam targeting businesses where a bad actor gains control of an employee's email account (typically within the finance department) and sends a fraudulent request for payment into an account controlled by the bad actor. To avoid becoming a victim, pick up the phone and verify the request by using existing contact information you have on file — never use contact information included in the email.

Cyber education and awareness are your best defense

Stay abreast of the latest cyber trends and emerging threats most common to your business/industry. Block time on your calendar each week where you can focus on reading about the most recent threats and how to prevent/mitigate against them. Allow your employees this time as well.

A knowledgeable staff can help detect and prevent cyberattacks. Train your employees on how to detect phishing emails and identify social-engineering scams. Instruct your employees to report any suspicious links and attachments to your information technology or information security department for analysis, if available.

Want to learn more?

Talk to your Wells Fargo investment professional today to learn more about the resources Wells Fargo has available to help you better protect yourself and your business from cybersecurity threats and financial fraud.

Wells Fargo provides best practice information related to cyber risk and/or topics for educational and information purposes only. This document is not intended to and should not be relied on to address every aspect of the risks discussed herein. The information provided in this document is for the purpose of helping customers and clients better protect themselves from cyber risk and highlight industry best practices for operating in a more secure manner. This document does not provide a complete list of all cyber threats or risk mitigation activities, nor does it document all types of best practices. Wells Fargo is not providing cyber-related advice or consulting services and customers and clients should decide whether to engage a cybersecurity firm for specific questions or advice. It is the responsibility of our customers and clients to determine their best approach for mitigating cybersecurity risk through implementation of best practice aligned to the level of risk.

Wells Fargo Wealth & Investment Management (WIM) is a division within Wells Fargo & Company. WIM provides financial products and services through various bank and brokerage affiliates of Wells Fargo & Company

The Private Bank is an experience level for qualifying clients of WIM. Bank products and services are available through Wells Fargo Bank, N.A., Member FDIC.

Wells Fargo Advisors is a trade name used by Wells Fargo Clearing Services, LLC (WFCS) and Wells Fargo Advisors Financial Network, LLC, Members SIPC, separate registered broker-dealers and non-bank affiliates of Wells Fargo & Company. WellsTrade® and Intuitive Investor® accounts are offered through WFCS.

© 2023 Wells Fargo Bank, N.A. CAR-0623-02779