

Make backup copies of important systems and data.
Regularly backup the data from computers used by your business. Remember to apply

the same security measures, such as encryption, to your backup data that you would apply to the original. In addition to automated backups, regularly backup sensitive business data to a storage device at a secondary location that is secure.

Pay close attention to your bank accounts and watch for unauthorized withdrawals. Put in additional controls, such as confirmation calls before financial transfers are

associated with theft if negligence on the part of your Businesses are generally not covered by federal directing the funds to the cyber criminal's account. electronic transfers made from bank accounts held authorized with the financial institution. In recent common scams, were factors in the loss may not be responsible for reimbursing losses consumer protections against unauthorized electronic forging payment requests for legitimate vendors and Business Email Compromise, targets businesses by and then make withdrawals. Another scam called the IDs and passwords for online bank accounts software, such as keystroke loggers, to obtain takeover where cyber criminals use malicious by businesses. A common scam is an account business, such as unsecured computers or falling for funds transfers. Therefore, your financial institution years, there has been an increase in unauthorized



Don't forget about tablets and smartphones. Mobile devices can be a source of security challenges. especially if they hold confidential

information or can access your business's network. If your employees connect their devices to the business's network, require them to password protect their devices, encrypt their data, and install security apps to prevent criminals from accessing the device while it is connected to public networks. Be sure to develop and enforce reporting procedures for lost or stolen equipment.



Watch out for fraudulent transactions and bills. Scams

can range from payments with a worthless check or a fake credit or debit card to fraudulent returns of merchandise. Be sure you have insurance to protect against risks. Additionally, ensure that you report any irregularities immediately.



Educate yourself. To learn more about protecting your business, visit the "Stop. Think. Connect." resources

for small businesses at https://www.dhs.gov/ publication/stopthinkconnect-small-business-resources



A Tradition of Trust

www.farmersstate.com

心である

A message from the Federal Deposit Insurance Corporation

FDIC-041-2015

A CYBERSECURITY GUIDE for Businesses



clear of fraudsters need to know how to steer are required to have vigorous attecting businesses and business customers also information security programs consumers are frequently tinancial institution to safeguard financial data, insured financial institutions in the news. While federally Computer-related crimes

customers on how to safeguard computer systems and data. cybersecurity information for Federal Deposit Insurance financial institutions' business Corporation, provides This guide, developed by the



policies for employees, such Establish security practices and Teach employees the basics as appropriate Internet usage

vital data. Ensure that all employees know how to cybersecurity, especially when it comes to handling culture that stresses the importance of strong identify and report potential security incidents. and protecting customer information and other for policy violations. Establish a top-down corporate guidelines, and set expectations and consequences

> access to the router by using strong passwords. make sure it is secure and encrypted. Protect update. If you use a wireless (Wi-Fi) network, set antivirus software to run a scan after each as appropriate, to keep it current. For example, complexity of your business. Update the software, vary, so find one that is right for the size and prevent unauthorized access. Protection options of information. Also, use a firewall program to consent for a variety of uses, including theft access a computer system without the owner's malware, or malicious software, which can antivirus software that protects against networks. Install security and Protect computers and



where and how they connect Train employees to be careful

relatively easy for cyber criminals to intercept the free Wi-Fi networks at public "hotspots." It can be connection they are using, as is the case with many network if they are unsure about the wireless employees shouldn't connect to your business's or public library, may not be secure. Also, your such as at an Internet café, hotel business center, trusted and secure connection. Public computers, parties should only connect to your network using a Internet traffic in these locations. to the Internet. Employees and third



Employees need to be suspicious of dangers of suspicious emails. Train employees about the

a reputable company or organization's logo into a matter how legitimate they appear. strategy is to ignore unsolicited requests, no installing malware on your network. The safest to be a simple request, your employees may be phishing e-mail. By complying with what appears information. It's easy for cyber criminals to copy on a link, open an attachment, or provide account unsolicited e-mails asking them to click



symbols that are hard to guess and changed and online accounts by using combinations of upper- and lower-case letters, numbers, and and passwords for computers, mobile devices. employees and other users connecting to your network use strong user IDs authentication. Ensure that Require strong

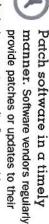
access systems or accounts. Control access to data and

computers and create user accounts for each employee.

to see if they offer multifactor authentication to Check with vendors that handle sensitive data information beyond a password to gain access

authentication that requires additional regularly. Consider implementing multifactor

personnel, have them and regularly review their administrative privileges, such as IT staff and key employees access to the specific data systems make sure that only employees who need install software without permission. Also, they need to do their jobs, and don't let them employees from sharing accounts. Only give be easily stolen or lost. Require each employee ongoing need for access. to have a separate user account and prohibit Lock up laptops when not in use as they can business computers to authorized individuals Take measures to limit access or use of



software to install such updates automatically. are available. It may be most efficient to configure install these software updates as soon as they products to correct security flaws and improve functionality. A good practice is to download and