Patch software in a timely manner. Software vendors regularly provide patches or updates to their products to correct security flaws and improve functionality. A good practice is to download and install these software updates as soon as they are available. It may be most efficient to configure software to install such updates automatically.

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

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.

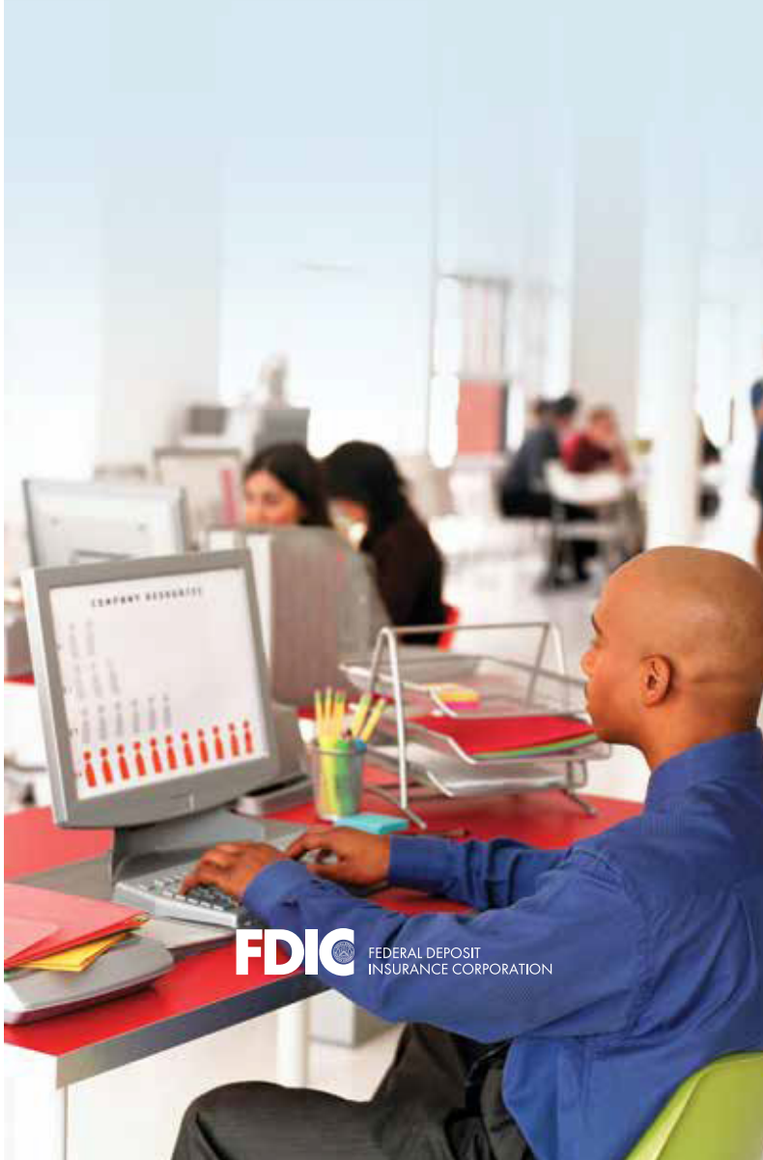
Watch out for fraudulent transactions and bills. Scams can range from payments with a worthless check or a fake credit or debit card to fraudulent returns of merchandise. Be sure you have insurance to protect against risks. Additionally, ensure that you report any irregularities immediately.

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 message from the
Federal Deposit Insurance Corporation

FDIC-019-2016

A CYBERSECURITY GUIDE for Businesses



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

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

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

Require strong authentication. Ensure that employees and other users connecting to your network use strong user IDs and passwords for computers, mobile devices, and online accounts by using combinations of upper- and lower-case letters, numbers, and symbols that are hard to guess and changed regularly. Consider implementing multifactor authentication that requires additional information beyond a password to gain access. Check with vendors that handle sensitive data to see if they offer multifactor authentication to access systems or accounts.

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

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

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

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