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