Cybersecurity for Small Businesses: Ways to Stay Protected

In today's world, it's important for small business owners to be vigilant in protecting their computer systems and data. Among the reasons: Federal consumer protections generally do not cover businesses for losses they incur from unauthorized electronic fund transfers. That means, for example, your bank may not be responsible for reimbursing losses associated with an electronic theft from your bank account — for instance, if there was negligence on the part of your business, such as unsecured computers or falling for common scams.

(To learn more about the rules pertaining to electronic theft, including losses involving a business debit card, go to the FDIC website and enter *fdic.gov/consumers/consumer/news/cnwin16/limit_losses.html*)

Here are tips to help small business owners and their employees protect themselves and their companies from losses and other harm. Several of these tips mirror basic precautions we have suggested elsewhere in this issue for consumers.

Protect computers and Wi-Fi networks. Equip your computers with up-to-date anti-virus software and firewalls to block unwanted access. Arrange for key security software to automatically update, if possible. And if you have a Wi-Fi network for your workplace, make sure it is secure, including having the router protected by a password that is set by you (not the default password). The user manual for your device can give you instructions, which are also generally available online.

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.

Set cybersecurity procedures and training for employees. Consider reducing risks through steps such as pre-employment background checks and clearly outlined policies for personal use of computers. Limit employee access to the data systems that they need for their jobs, and require permission to install any software.

And, train employees about cybersecurity issues, such as suspicious or unsolicited emails asking them to click on a link, open an attachment or provide account information. By complying with what appears to be a simple request, your employees may be installing malware on your network. You can use training resources such as a 30-minute online course from the Small Business Administration (SBA). To review the course, go to the Small Business Administration website and enter *sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses*

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 requiring more information beyond a password to gain access to your business's network, and additional safety measures, such as requiring confirmation calls with your financial institution before certain electronic transfers are authorized.

Secure the business's tablets and smartphones. Mobile devices can be a source of security challenges, especially if they hold confidential information or can access your company's network. In the case of the latter, require employees 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. Also develop and enforce reporting procedures for lost or stolen equipment.

Back up important business systems and data. Do so at least once a week. For your backup data, remember to use the same security measures (such as encryption) that you would apply to the original data. In addition, in case your main computer becomes infected, regularly back up sensitive business data to additional, disconnected storage devices.

Use best practices for handling card payments online. Seek advice from your bank or a payment processor to select the most trusted and validated tools and anti-fraud services. This may include using just one computer or tablet for payment processing.

Be vigilant for early signs something is wrong. "Monitor bank account balances regularly to look for suspicious or unauthorized activity," suggested Luke W. Reynolds, chief of the FDIC's Outreach and Program Development Section.

***Information is provided by the Federal Deposit Insurance Corporation – FDIC -019-2016*