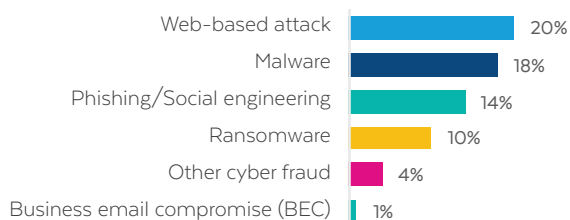# Security

Ensure you have the most up-to-date security protection for your business technology platforms.

Why does security matter?

Security protection is important for any business, but especially for small businesses. Small businesses tend to see more attacks since they often have less scale and fewer security resources than larger companies. Protecting physical hardware, software and data means having the most up-to-date security protection for all business technology platforms. Education about potential security threats and vulnerabilities, both offline and online, is critical for you and your staff.
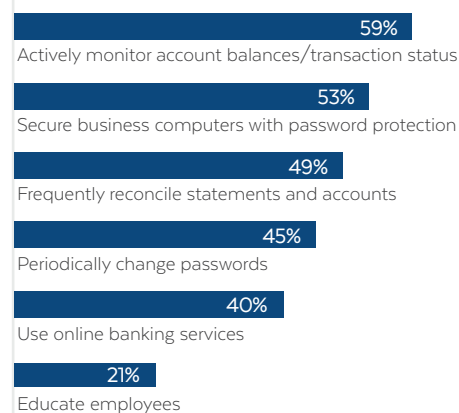
What types of attacks did your business experience?[1]
% of attacked small businesses experiencing type of fraud:

Web-based attack	20%
Malware	18%
Phishing/Social engineering	14%
Ransomware	10%
Other cyber fraud	4%
Business email compromise (BEC)	1%

Actions taken to defend against attacks that would compromise security[1]
% of small businesses that have implemented this action:

Actively monitor account balances/transaction status	59%
Secure business computers with password protection	53%
Frequently reconcile statements and accounts	49%
Periodically change passwords	45%
Use online banking services	40%
Educate employees	21%

Key actions to take:

Protect your business from the risks of an online attack with well-thought-out prevention measures.

- **Secure your hardware**: Securing computers and routers from physical and cyberattacks is a first step. Implement password protection for all devices and networks. An unprotected router is an invitation for online hackers to troll outgoing and incoming traffic to your business. Open routers can also slow down your Internet access and affect your ability to do business because of bandwidth saturation. Network security using Virtual Private Networks (VPN) technology can provide a much higher level of security without restricting access for those who need it. Make sure all data is encrypted, particularly on laptops and mobile devices, and that you have the means to isolate or erase files on stolen devices.

- **Secure your software**: Stay current with software updates for both your computers and routers. Updates for operating systems and firmware address security vulnerabilities and provide the latest security patches against malware and other cyberattacks. Applications, such as the ones you use for financial management, invoicing and point of sale (POS), will have periodic updates as well. Install the latest updates when they are available to stay protected.

- **Educate yourself and employees**: Set up training sessions for employees where they can learn about cybersecurity and other vulnerabilities. Cover the security measures you have in place and expectations towards defending against cyberattacks. Include a section on being secure while online. Many people inadvertently make themselves vulnerable with their activities online by using a non-secure Wi-Fi source, providing personal information on an unsecured site, or opening emails with

malware. Establish guidelines on data release and set up procedures for staff data access.

- **Implement virus protection software**: Virus protection software is an easy, inexpensive way to secure your computers and network. The software will help you to prevent malicious emails, links and documents from infecting your computers. Cyberattacks are always advancing and changing, so be diligent in updating your virus protection software to protect against new forms of attacks.

- **Consider data security**: Many businesses store confidential data ranging from payment details to customer names and information about business relationships. Exposure of this data could cause irreparable damage to your customers and to your company. Set explicit procedures on how this data can be shared securely within your company. Whether you keep data within a company network or use file-sharing services with proper encryption and password protection, make sure you limit access to those who need it and educate your staff on the proper transmission and sharing of confidential data.

Click below for additional resources:

Fraud Tip: Implement Disaster Planning
Create a recover plan to protect against emergencies and allow you to recover quickly.

Infographic: Small Business, Big Risk
Learn about the risks of cyberattack.

How can SunTrust help you?

- Drop by your SunTrust branch
- Call us at 800.752.2515
- Visit suntrust.com/bizbestpractices

SunTrust®