Protect your business

It seems on a daily basis we read about cyberattacks in the news. It's not just the big, global companies that experience them either. According to a 2017 Keeper Security and Ponemon Institute report, about 61 percent of small and medium-sized businesses experienced a cyberattack in the last 12 months. Many of these attacks are completely preventable by using simple, fundamental security practices.

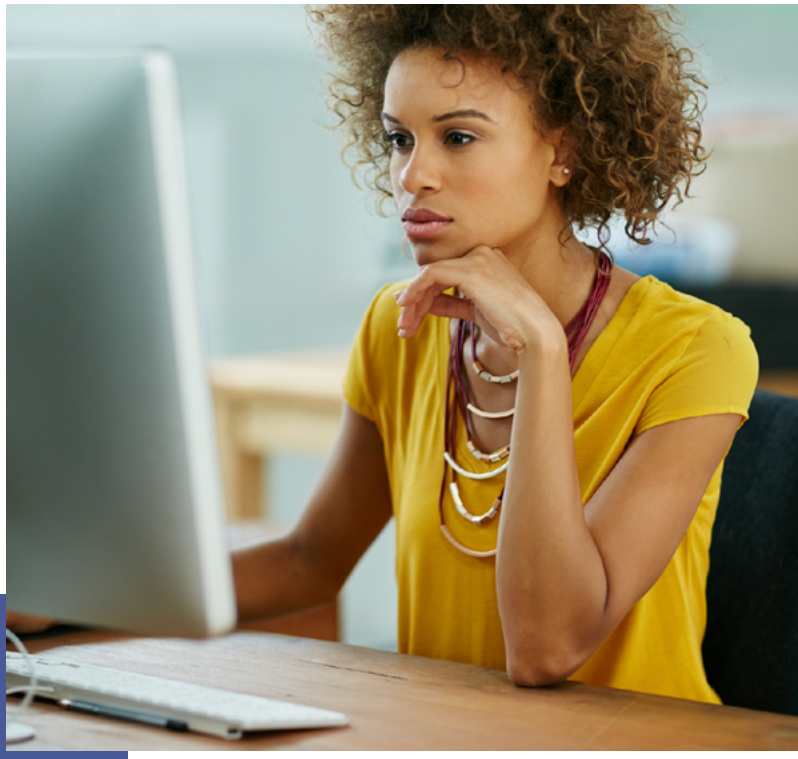
Whether large, medium, or small, the following tips can be used by any business to help mitigate the risk of a major cyberattack.

It all starts with training.

- Everyone who touches your business' computer network—including employees, contractors and vendors—needs to receive training on computer security awareness and how to avoid becoming a victim of common cybercriminal schemes. This will ensure that standard cybersecurity practices become a part of your company's culture. According to Kroll, an information management firm, 31 percent of organizations say employee negligence is the root cause of data breaches.
- Your mandatory cybersecurity training should be conducted on a periodic basis and should be updated regularly as some threats, such as ransomware, phishing, social engineering, and business email compromise (BEC) are on the rise.

A note on BEC

- In a BEC scheme, cyber criminals target employees who have access to company finances. The cyber criminals then lure these employees via fake emails appearing to be from an authorized company official into making wire transfers to accounts managed by the criminals.
- According to the FBI, between early 2015 and late 2016, the agency observed more than a 2,000 percent increase in losses associated with BEC.



- Along with awareness training, having a "second-look" procedure or requiring more than one person to approve a wire transfer, will give your company a better chance of spotting suspicious transactions.
- Employees should also learn how to report potential incidents to the appropriate company officials, even if they don't know if the threat is real or not. Better safe than sorry.

Develop strong policies.

- Having official policies on paper that all employees, contractors, and vendors are expected to adhere to, make it easier to actually enforce compliance with standard cybersecurity practices.
- The National Institute of Standards & Technology (NIST) Cybersecurity Framework is a good starting point for guidance on how to create policies as a part of your overall risk management strategy. For more information visit: www.nist.gov/cyberframework

Secure your network.

- As a first line of defense, it is suggested to have hardware and software firewalls installed to protect your network. Firewalls monitor incoming and outgoing traffic and will either allow or block traffic based on your security rules.
- No network protection is complete without good anti-virus software. Anti-virus software helps to detect and remove viruses, and other malicious software.

- Be sure there's a plan in place to ensure all security updates and patches from your software providers are installed on all workstations and devices within a reasonable timeframe.
- Remote or virtual employees should be provided access to a Virtual Private Network (also known as a VPN) to log in to your network securely regardless of their location. If you provide Wi-Fi access on-site, make sure it is password protected and configured securely.
- If two-factor authentication (i.e., having two different sets of credentials to login) is an option for your network or your systems, enable it. An example of two-factor authentication would be a user receiving a Personal Identification Number (PIN) sent via text message and then using that PIN in conjunction with a user ID and password.

Go the extra mile.

- On a periodic basis, conduct an assessment of the cyber risks facing your organization. Whether it's handled internally by company leadership or employees who are closest to your cyber vulnerabilities, or even by an outside cybersecurity firm, cybersecurity risk assessments all begin with the same question: What are the company's top cybersecurity risks?
- Have a plan for recovery. In the event of a cyberattack, your company needs a plan in place on how normal operations will be restored. Your plan should also address what happens if your company is indirectly affected by a cyber incident from a third-party. Your plan should be exercised on a periodic basis to identify any gaps and make improvements. Being prepared for the worst will help ensure a quicker recovery, with less business impact.
- Consider obtaining cyber insurance. Just like your personal insurance can cover losses from vehicle theft or a house break-in, cyber insurance is a product that can help mitigate the costs associated with a cyber incident whether it results in data loss or loss of funds. According to the Keeper Security and Ponemon Institute report, disruption to operations due to a cyberattack costs small and medium-sized businesses an average of nearly $1 million and they spend an average of $900,000 due to damage or theft of their information technology assets.
- Back up your data. In the event of a ransomware or destructive malware attack, your time to recovery is critical in reducing any possible financial losses. Data backup will provide your business with a "point-in-time" snapshot of your data which may help speed up recovery efforts. Depending on the size of your business, data backup can be as straightforward as periodically capturing your data on offline media such as discs or removable storage devices; and may include other options such as network attached storage or online solutions such as a private cloud or an online storage service. It is also important to verify that your data backups are clean from infections.

This list of suggestions will help you get started or continue on your journey to securing your business, regardless of size. Please see the following resources for further help with protecting your business:

- **To report suspicious activity or fraud to U.S. Bank**
  www.usbank.com/online-security/report-suspicious-activity.html

- **Department of Homeland Security Voluntary Program**
  www.us-cert.gov/ccubedvp

- **Federal Bureau of Investigation Cyber Division**
  www.fbi.gov/investigate/cyber

- **Department of Homeland Security Cyber Security Awareness Campaign**
  www.stopthinkconnect.org

- **Federal Trade Commission Privacy and Security Site**
  www.ftc.gov/tips-advice/business-center/privacy-and-security

- **Global Cyber Alliance**
  www.globalcyberalliance.org

- **National Council of Information Sharing and Analysis Centers**
  www.nationalisacs.org