Dollar Bank

# Business Insights

## Data Breaches & Other Cyber Threats:
Protecting your company information and networks is essential to your success

- Common Cyberattack Threats
- Tips for Protecting Your Business

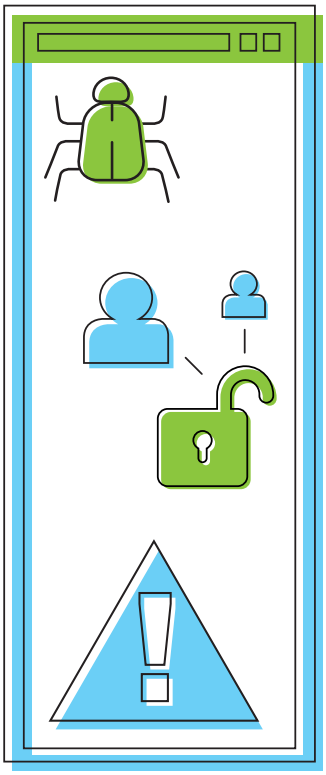
**When data that company leaders thought was secure is suddenly exposed to unauthorized users, chaos can ensue. We've all heard of major data breaches that have put companies out of business or caused them to pay restitution to customers whose personal information, passwords, account numbers or other data were compromised in an attack or an unintentional data leak. Breaches involving the exposure of intellectual property, proprietary processes, confidential legal issues and the like can be equally harmful.**

Although the news might report only on compromises to large corporations, smaller businesses are targets, too. In fact, the 2019 Data Breach Investigations Report by Verizon states that 43% of data breaches target small businesses. These breaches can be costly to a company's reputation as well as its financial standing.

Prevention begins with knowledge. This whitepaper offers basic information about data breaches and other potential threats to your computer networks, systems, infrastructure and devices.

## Common Cyberattack Threats

Malware, social engineering, denial-of-service, man-in-the-middle and password attacks are among the most common cyberattacks waged against businesses. Be aware, however, that there are many other types of attacks, often involving complex hacking tactics that require intervention by IT security professionals.



- ***Malware Attacks:*** Malware is harmful (malicious) software installed onto a system when unwitting users click illegitimate links or attachments, or when a hacker exploits network vulnerabilities. Malware takes a variety of forms — viruses, worms, ransomware, spyware and adware — and may cause damage such as blocking access to the network, copying and transmitting data from a hard drive, disrupting or disabling a system, etc.

- ***Social Engineering Attacks:*** Social engineering ploys con users into inadvertently providing access to sensitive data or to the network itself. Phishing is the most widely used social engineering tactic, as scammers send e-mails that appear to come from a trusted source — an employee's manager or an HR representative, for example. They generally ask the recipient to click a link, download an attachment or take some other action that provides access to the network or accounts within it.

- ***Denial-of-Service (DoS) Attacks:*** DoS attacks involve flooding a targeted network with traffic, overwhelming it to the point of being unable to respond to requests for access by legitimate users. Customers may be unable to make online payments, for example, or to get through to your website. Employees also may be unable to access their work e-mail accounts.

- ***Man-in-the-Middle (MitM) Attacks:*** Also known as eavesdropping attacks, MitM attacks involve a cybercriminal who intercepts communications between a legitimate user and the network. Often leveraging unsecure public Wi-Fi when an employee is working remotely, the attacker might breach a device with malware so that all information the user believes they are sending to the network is stolen along its way.

- ***Password Attacks:*** Although users are becoming savvier about the passwords they choose, and more companies are investing in password managers to safely generate and retrieve strong, random passwords, attackers still find vulnerable accounts where they can crack the password code to rob individuals and companies of confidential information. They may do this by systematically guessing, using social engineering tactics or gaining access to a password database.

## Tips for Protecting Your Business

The most recent Ponemon Institute Cost of a Data Breach Report (2017) shows that the longer it takes for a company to detect a data breach, the more expensive it will be. On average, U.S. companies take 206 days to detect a breach. That's a lot of time for a cybercriminal to be poking around your network. Diligence in implementing security measures and monitoring your systems is vital. Some suggested measures follow.

- ***Update at every opportunity.*** The operating system, software, browsers and plugins used at your company should be updated as soon as updates, including vital security patches, become available.

- ***Train your staff.*** Heightened security awareness among employees is critical to protecting your business. Here are some essential actions they should take:

  - Knowing the red flags of phishing e-mails and other social engineering ploys (and never clicking on links or attachments from unknown sources)
  - Managing their passwords, including creating strong passwords and changing them frequently
  - Protecting their devices — smartphones, desktops, laptops and any other devices connected to the company network — from physical loss or theft
  - Reporting any suspicious activity to the appropriate point person


**of data breaches target small businesses**

*Source: 2019 Data Breach Investigations Report, Verizon*

### Actions Causing Data Breaches

**Hacking ..... 52%**

**Social Attacks..... 33%**

**Malware..... 28%**

**Errors ..... 21%**

**Misuse by Authorized Users..... 15%**

**Physical Actions *(e.g., device theft)*..... 4%**

*Source: 2019 Data Breach Investigations Report, Verizon*

**Average time it takes for a company to detect a data breach**


*Source: 2017 Cost of a Data Breach Report, conducted by Ponemon Institute and sponsored by IBM Security*

DollarBank®

- ***Protect your network, data and devices.*** It makes sense to stay apprised of available technology solutions and to put policies into place to enhance your security:

  - Consult an IT expert to determine what layers of security your system requires, beginning with a strong firewall and antivirus software, as well as encryption software to render any stolen data useless to the cyberthief. Ask them about vulnerability scanning and penetration testing.
  - Limit the number of devices connected to your network.
  - Limit access to sensitive data to designated employees.
  - Implement an account lockout policy that permits only a few password attempts at login, and consider investing in password management technology.

- ***Create a disaster recovery plan.*** Even the strongest security measures can sometimes be compromised. Have a written plan in place to ensure successful and efficient communication, damage mitigation and data recovery in the event of a cyberattack.