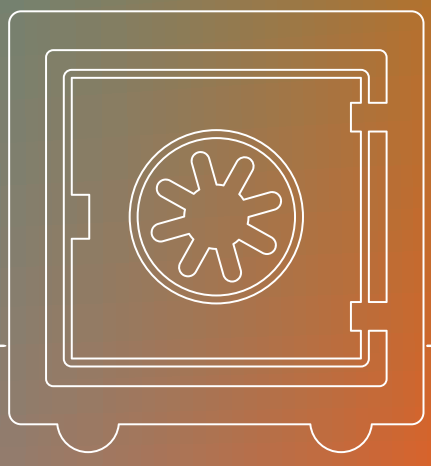
dashlane business

2017 Guide to Password Management for Small Businesses

4 Cyber Threats Targeting Small Businesses in 2017



It's too dangerous for organizations of all sizes to put the issue of cybersecurity on the backburner in 2017. The National Cyber Security Alliance survey found that 66 percent of small business owners are not concerned about external threats (like hackers or data leaks) or internal threats (like an ex-employee or contractor stealing data). It's this false sense of cybersecurity that leads to 60 percent **of hacked small businesses to go out of business within six months of a cyber-attack.**

Fortunately, some steps that go a long way toward protecting a company — such as employee education and password protection — are relatively inexpensive.

The first move toward keeping hackers out of company files and assets is to know the major problems on the horizon. That includes an awareness of the leading cyber threats targeting small businesses in 2017:

- Social engineering, including phishing and spear phishing
- Password attacks
- Denial of service (DoS) and distributed denial of service (DDoS) attacks
- Infection with ransomware

Social **Engineering**

Hackers are always looking for vulnerabilities in systems of company information, but not all weaknesses are part of a company's digital systems. **Oftentimes, a cyber criminal's main target are the employees of an organization or small business**, including company executives, managers, and employees who are too trusting when receiving requests for sensitive information whether by email, text message, or phone.

This is **social engineering** — a technique used to retrieve important/sensitive information by manipulating the target. Two leading forms of social engineering attacks come through phishing and spear phishing emails in which a sender's name and subject line appear legitimate.

Phishing

A phishing email is sent to many people in hopes that at least a few will fall prey to it. Sometimes phishing is easy to identify because (1) it appears to come from a person or organization with whom you have little or no connection, (2) the subject line sounds strange, or (3) the email contains links or attachments from a purported sender who you probably don't know.

Spear Phishing

In contrast to the broad net cast by simple phishing, a spear phishing email is tailored to one or a few recipients. It is carefully based on information about your life, work, or interests that cybercriminals can easily find on social media profiles, public resumes, and other sources.

A truly crafty cybercriminal may use the names and even the addresses of your friends and colleagues. These email spoofs are harder to identify, but may accidentally include a clue, such as an unusual request. They may also allude to a compromised account and request a password change, as in the famous email that sank John Podesta, the former Democratic campaign chair for Hillary Clinton.

Here's another example, with a huge dollar sign attached: network technology company, Ubiquiti Networks, lost $46.7 million to spear phishing in 2015 when a cybercriminal targeted the company's finance department and impersonated an employee. The Infosec Institute reports that the pseudo employee requested fund transfers by using "spoofed email addresses and look-alike domains" that the crook found online.

Invest in **Phishing Filters** and "**Human Firewalls**"

At the most basic level of cybersecurity, companies need to use browsers with built-in phishing filters that are enabled for all users. Mozilla Firefox, Google Chrome, and Microsoft Internet Explorer provide anti-phishing and anti-malware protections in the privacy settings.

In addition, "human firewalls" form a major defense against hacks; your employees need to receive training about how to vet the safety of emails. Every employee should also know how to check an email's source and how important it is to maintain heightened awareness of strange requests, suspicious attachments, and anything that doesn't sound right.

Equip your "human firewall" with these essential tips from our guide for preventing phishing scams:

- Check the validity of the sender by hovering the computer's mouse (or a finger on the trackpad) over the sender's name. A box will pop up showing the actual email address it came from.
- If the email is opened, hover over any links to look for suspicious mail paths, but never click on them.
- Unfortunately, identification of the URL connected to an email can be difficult on a smartphone. So, never open any links within a questionable email on a smartphone or tablet. Wait to check its URL on a computer.
- When scrutinizing an email on any digital venue, keep in mind other clues hinting of deception, such as odd wording, misspellings and urgent language requesting you to take an action requiring sharing private information.
- Tell staff that if doubt still lingers, they shouldn't open the attachment until they have checked with the person or organization that purportedly sent the email, or IT personnel.

Password **Attacks**

Verizon's 2016 Data Breach Investigations Report **(DBIR) noted that weak or stolen passwords were the source of 63 percent of data breaches last year.** The DBIR also reported that 95 percent of these password-related cyber-attacks were financially motivated. In addition to financial firms, other organizations hit hard by password attacks were in the healthcare, hospitality, information, public, and retail sectors.

Password attacks taking advantage of weak or reused passwords are the result of risky password practices employees use on their personal accounts, and inadvertently transfer into the workplace.

Poor password practices

Passwords may be weak for many reasons, including:

- Using simple, easy-to-crack number combinations (i.e. "123456") and phrases (i.e. "starwars" or the ever popular "password")
- Containing identifiable dictionary words, curse words, names, places, etc. instead of random strings of letters, numbers, and symbols
- Reusing one or more passwords across many online accounts
- Recycling parts of old passwords instead of creating entirely new combinations
- Never changing the manufacturer's default passwords that come with a device or software
- Sharing passwords between employees via email, text messages, Sticky notes, Word documents, etc. (Password sharing is particularly dangerous when it involves access to privileged accounts, such as data that shouldn't be shared outside your company.)

Password-Cracking Strategies

Once hackers have broken into a company's computers, they may use strategies such as brute force, dictionary, or keylogger attacks to identify passwords and crack ones that are encrypted.

Brute Force is a try-try-again method of decoding password possibilities via an automated computer program. Starting at one-digit passwords and moving on to longer combinations of letters, numbers, and symbols, this strategy calculates possible combinations.

Dictionary Attacks are based on the idea that people love using words, names, places, slang, etc. in passwords. This technique relies on an automated computer search based on common dictionary words.

Keylogger Attacks are much different. First, a hacker needs to find a way to implant malware in the target's computer system. The hacker might do this by including keylogger code in an attachment in a spear phishing email. Once installed, a keylogger program tracks and records every keystroke of the computer user; this program can be used to record not only login credentials, but also your credit card information, social security numbers, phone numbers, and more.

Password Protection

Password management programs are the fastest and most effective way to clean up employee password use and tighten company security. When employees use a password manager, they no longer need to remember their passwords; the program does it for them.

Each employee's account is like a separate bank vault. The contents of the vault are secured through the processes of encrypting and salting. Many password managers also support multi-factor authentication, which makes it impossible to open the vault without a code sent to the employee's smartphone or a security token like a YubiKey.

Denial-of-Service Attacks

Denial-of-service attacks hit businesses of all sizes. According to the National Cybersecurity Institute, **by the third quarter of 2015, DDoS attacks on small businesses increased 180 percent over the previous year.**

In October 2016, Fortune noted that while politics and revenge motivate some DDoS attacks, many are focused on financial gain through blackmail and industrial sabotage. Said Fortune: "Companies seeking to undermine their competition can hire hackers to take the other guys offline."

SMBs don't have deep pockets. Denial of service causes them to lose income and customer loyalty during and following attacks. Among other problems, their bond ratings may be downgraded and they may need to expend sizeable funds on reputation damage repair.

Strong password control of IoT (Internet of Things) systems would be a major step toward making malware infection and DDoS tougher to achieve.

Extortion via **Ransomware**

When online criminals sneak malware code into a company's database files, costly extortion usually is the intent.

Cybersecurity often takes a backseat to other business development for SMBs despite being inexpensive relative to cybercrime. In addition to adding firewalls and keeping anti-virus software updated, New York Times reporter Constance Gustke noted, small businesses can store data with cloud service companies, like Dropbox or Google Drive. She added that the cloud is less vulnerable than a small company's own servers.

"Among the simpler precautions small businesses and consumers alike can take is to create strong passwords," Gustke wrote. "That has long been the advice of security experts but many say it is stunning how many people and small businesses fail to heed the advice."

Business **Protection Tips**

Company protection begins with a solid cybersecurity plan that provides procedures for all staff to use in identifying and reducing cyber threats.

The plan should include regular employee education about how to follow its procedures, recognize threats, and report cyberattacks to management. Monthly town hall meetings and employee newsletters are great communication tools.

Other measures we recommend to limit cyber-attacks include:

- Using an email filtering system to detect phishing schemes, ransomware, spam, malicious attachments, etc.
- Avoiding vulnerability by updating computer systems with patches from software producers
- Monitoring all devices and applications connected to the company network, especially BYOD (bring your own device) and mobile devices
- Installing a strong firewall and anti-virus/anti-malware software
- Including any IoT devices in an encrypted Wi-Fi network

Finally, to echo The New York Times, everyone on staff needs an individual account in the company's password management program.