How-to guide:
Step up your company’s cyber defenses
How-to guide: Step up your company’s cyber defenses

The risk of your business being hacked has never been higher. Cybercrime is now the second most common type of economic crime reported by companies, according to a 2016 report, and small businesses are a prime target. Use this guide to safeguard your assets by knowing current threats, sound technology practices, and the role your team can play in defending your business.
Defend your business by learning what criminals know

*Big-company data breaches make the news, but recent cyberattack statistics show that cybercriminals are increasingly focused on small businesses. Avoid becoming their next victim by learning the types of crimes currently in play and how crooks operate.*

Cybercriminal threats fall into a few major categories:  

**Ransomware** is a type of malicious software that blocks access to data by encrypting files until a sum of money is paid. It’s become the most widespread type of malware afflicting businesses, and because it’s also the most profitable, it’s expected to increase.

**Data breaches** are instances of criminals accessing or stealing confidential information from your company by infiltrating a mobile device, website, server, or other piece of technology. This type
of crime is at its highest point ever, and hitting companies harder: A 2016 study reports that the average breach costs businesses 29 percent more than it did three years ago.

Bank fraud may have the most immediate effect on businesses’ bottom lines, since funds can be transferred electronically within seconds. In these scams, hackers often impersonate a company official over email in their attempts to obtain funds, usually by falsifying an order to transfer money out of the business’s accounts.

You may picture a cybercriminal as a technology wiz, but old-fashioned con-artist tricks are often the key to breaching information security defenses. Educate yourself and your team to be alert for these tools of the trade:

- **Social engineering.** This ploy preys on employees’ misplaced trust, often in a bogus caller or faked email asking for login information. Some fraudsters will impersonate senior managers or other executives who need a password reset. One successful ploy sent “unusual account activity emails” to Gmail users asking for a password reset.

- **Malvertising.** Malware is spread via advertisements and websites, and infiltrates victims’ computers and networks to steal protected information. A related tool is “rogue mobile apps” that tap protected information such as login and other material through a mobile device.
• **Rogue mobile apps.** These are often disguised as legitimate applications to trick you into downloading them, but are laden with malware designed to access your personal and corporate data, including passwords.

• **System vulnerabilities.** Attackers probe for outdated software and hardware, as these are particularly likely to contain security flaws, glitches, or weaknesses that can provide entry points.

### 4 ways to boost your defenses

1. **Keep your technology current.** Your software and hardware systems will be better protected when you keep them current with any updates or patches provided by the manufacturer. Set your systems to automatically download software updates, and make it company policy to install them immediately. Consider migrating off of old software that no longer receives software updates and old routers that do not get firmware updates.

2. **Use security tools.** Most small businesses don’t have the resources to keep an information security specialist on staff, but there are many options for getting outside help. One of the most important technology countermeasures is installing a network firewall and good antimalware tools. Services such
as Avast and McAfee® Endpoint Protection with AT&T will help protect Windows devices. If malware gets through despite your efforts, you can get help with removing spyware and viruses from AT&T Tech Support 360SM.

3. **Back up your data at least daily.** Remember that your data is one of your most important business assets, so plan for the possibility that a ransomware attack could put critical files out of reach. Offsite data services such as Carbonite and AT&T Tech Support 360SM Backup and Go allow you to schedule automatic backups and offer mobile access to cloud-based storage.

4. **Train your team.** No security strategy is complete without a plan to regularly educate users to recognize and guard against cyber threats. The National Cyber Security Alliance offers resources to businesses as part of its StaySafeOnline campaign, including advice on employee training. You can start by sharing the following checklist, “Teach your team cyber-safe habits,” with all your employees.
Teach your team cyber-safe habits

*When all team members follow sound cybersecurity practices, they’ll help protect company assets.*

After updating your team on common threats and cybercrime techniques, share this checklist with them. Consider holding a meeting to share these practices and post these tips prominently in your office as a reminder of good habits.

- **Beware email scams.** Only open email attachments that you’re expecting from senders you know, and check first via a phone call if you’re suspicious that a contact’s email account may have been taken over by an attacker. Never click a suspicious link without double-checking its destination, and don’t enter account credentials unless you have initiated the login.
Practice safe browsing. Keep your web browser and any plug-ins it uses up-to-date to prevent infection by malicious code. Visit only trusted websites and be wary of content you download; malware often lurks in images and video files on unscrupulous sites. When accessing or sending sensitive information, look for the HTTPS prefix in URLs, which signifies secure and encrypted communications.

Use tougher passwords. Use different passwords for all your accounts, choosing combinations of numbers, uppercase and lowercase letters, and special characters. (Adopting a password management tool such as LastPass makes it easier to keep many logins straight.) Use two-factor authentication for business applications and website logins for an added layer of security.

Protect your smartphone. Download only apps vetted by your device’s primary app store to reduce the risk of installing malicious code. Set up automatic updates so your operating system, anti-malware software, and applications are better protected. Follow your company’s mobile device policy, which may bar storing or transmitting sensitive company information with your mobile device.

Guard the physical security of your devices. Be aware of where your laptop, mobile phone, tablet, and other devices are at all times, especially when
you’re working remotely or traveling. Never leave your device unattended, even in your vehicle. Should your device be lost or stolen, follow company practices, which may include alerting your manager and remotely wiping all the data on your device.

- **Recognize social engineering attempts.** Criminals may try to fool you to gain access to company systems. Watch out for pop-ups or emails that ask you to enter your username and password to gain access to an application or site, or phone calls and emails in which the attacker impersonates a manager seeking sensitive company information. Take similar care with text messages and social media, and verify the identity of the person contacting you before divulging information.

- **Use public Wi-Fi with care.** Public Wi-Fi networks at coffee shops, hotels, or airports may be convenient for quickly checking your email, but they are notoriously unsecured. Accessing them leaves your devices and data susceptible to hackers. Be smart about the websites you access on public Wi-Fi: Avoid logging into online banking sites or business sites that hold sensitive information.