FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Small Business Computer Security Basics

TAGS: Privacy and Security | Data Security | Appliances | Automobiles | Clothing and Textiles | Franchises, Business Opportunities, and Investments | Human Resources | Jewelry | Non-Profits

If you're running a small business with only a few employees, you've learned about a lot of things – accounting, marketing, HR, you name it. And you probably depend on technology, even if it's only a computer and a phone. You can't afford to get thrown off-track by a hacker or scammer.

Here are a few computer security basics to help your company, even if you're the only employee. If you have employees, train them to follow these tips. If you collect any consumer information, also check out our advice about protecting personal information.

PROTECT YOUR FILES & DEVICES

Keep your software up-to-date. No matter what operating system, browser or other software you use, keep it up to date. Set it to update automatically so you don't leave holes hackers can exploit.

Back up your files. No system is completely secure. Create offline backups of important files. That way, if your computer is compromised, you'll still have access to your files.

Use strong passwords. The longer the better – at least 12 characters. Complexity also helps strengthen a password. Mix numbers, symbols, and capital letters into the middle of the password, not at the beginning or end. Don't use patterns to lengthen a password. Never use the same password for more than one account, or for personal and business accounts. If you write them down, lock them up. Consider using a password manager, an easy-to-access application that allows you to store all your valuable password information in one place. Be sure to protect your password manager with a strong master password, and only use a password manager from a reputable company. Don't share passwords on the phone, in texts or by email.

Turn on two-factor authentication. For accounts that support it, two-factor authentication requires both your password and an additional piece of information to log in to your account. The second piece could be a code sent to your phone, or a random number generated by an app or a token. This protects your account even if your password is compromised.

Don't leave your laptop, phone or other devices unattended in public, even locked in a car. They may contain sensitive information – and they're costly to replace. If they go missing, the information stored on them

may fall into the hands of an identity thief. You also can turn on device encryption to encrypt all data on each device. This reduces the risk to sensitive information in case your device is stolen or misplaced.

Password protect all your devices. If you access your business network from an app on your phone or tablet, use a strong password for the app, too.

THINK BEFORE YOU SHARE YOUR INFORMATION

Protect account information. *Every time* someone asks for business information – whether in an email, text, phone call or web form – think about whether you can really trust the request. Scammers will say or do anything – or pretend to be anyone – to get account numbers, credit card numbers, Social Security numbers or other credentials. Scammers will rush, pressure or threaten you to get you to give up company information.

Only give sensitive information over encrypted websites. If your company is banking or buying online, stick to sites that use encryption to protect your information as it travels from your computer to their server. Look for **https** at the beginning of the web address in the address bar of your browser. Look for https on every page of the site you're on, not just where you log in.

PROTECT YOUR WIRELESS NETWORK

Set up your router securely. If your small business has a wireless network, your "access point" is probably a cable or DSL modem connected to a wireless router, which sends a signal through the air. Your router directs traffic between your local network and the internet. Any device within range can pull the signal from the air and access the internet. If you don't secure your router, strangers could easily gain access to sensitive personal or financial information on your devices.

- ***Change the name of your router from the default.*** The name of your router (often called the service set identifier or SSID) is likely to be a standard, default ID assigned by the manufacturer. Change the name to something unique that only you know. Visit the company's website to learn how to change the router name.
- ***Change your router's pre-set password(s).*** Hackers know the default passwords, so change yours to something only you know. The same goes for any default "user" passwords. Use long and complex passwords. Visit the company's website to learn how to change the password.
- ***Keep your router's software up to date***. Before you set up a new router, and periodically thereafter, visit the manufacturer's website to see if there's a new version of the software available for download. To make sure you hear about the latest version, register your router with the manufacturer and sign up to get updates.
- ***Turn off any "remote management" features.*** Some routers offer an option to allow remote access to your router's controls, such as enabling the manufacturer to provide technical support. Never leave this feature enabled. Hackers can use them to get into your network.
- ***Log out as administrator.*** Once you've set up your router, log out as administrator, to lessen the risk that someone can piggyback on your session to gain control of your device.

Use encryption on your wireless network. Encrypt the information you send over your wireless network, so that nearby attackers can't understand your communications. Encryption scrambles the information you send into a code so that it's not accessible to others. Modern routers offer WPA2, the strongest wireless encryption widely available. To protect your data, use it.

Wireless routers often come with the encryption feature turned off. You must turn it on. The directions that come with your router should explain how. If they don't, check the company's website.

Limit access to your network. Allow only specific devices to access your wireless network. Wireless routers usually have a mechanism to allow only devices with particular unique Media Access Control (MAC) address to access to the network. If you want to provide free Wi-Fi for your customers, set up a second, public network – separate from the network for your business devices.

BE CAREFUL WITH WI-FI HOTSPOTS

If you're on the go, Wi-Fi hotspots in coffee shops, libraries, airports, hotels, and other public places are convenient – but often they're not secure. In fact, if a network doesn't require a WPA2 password, it's probably not secure. To protect your information when using wireless hotspots, send information only to websites that are fully encrypted – look for **https** on every page. And avoid using mobile apps that require sharing personal or financial information over public Wi-Fi.

KNOW WHAT TO DO IF SOMETHING GOES WRONG

Plan ahead so you know what to do if a hacker gets into your system. There are steps you can take to minimize the damage if you discover malware on your computers, that your email has been hacked, or even if someone takes over your system and demands a ransom to return control of it.

And if someone accesses personal or financial information that they shouldn't, take steps to respond to that data breach.

April 2017

ftc.gov