Data Security Checklist: Small Businesses

Office of Neighborhood Involvement Crime Prevention Program • portlandoregon.gov/oni/cp • March 2017

According to the National Cyber Security Alliance, 83% of small businesses do not have a formal cyber security plan (2012). Unless businesses take the necessary precautions, they will be more vulnerable to data breaches placing their employees, customers and business at risk. The financial liability associated with a breach can temporarily or permanently disrupt business operations. By having a plan, you will be less vulnerable and more resilient. Below is a list of basic considerations.

Activate firewalls and install anti-virus, anti-malware and anti-spyware software. Your Internet service provider may provide free software that you can download. • Virus software should be updated and run weekly, at a minimum.	
Update software immediately. Security breaches may occur through vulnerabilities in software. Hackers learn about the security flaws that are patched with an update and attempt to exploit those vulnerabilities with companies that haven't updated. • Keep software updated and stay informed about the latest security features and vulnerabilities.	
Create strong passwords. Weak passwords are the easiest way to infiltrate a computer network. Do all employees create strong passwords that are long and unique? Create a firm policy for employees and managers that includes the following recommendations: • Do not use the same user IDs and passwords for work and home accounts. This way the company will not be at risk if an employee's personal accounts are breached. • Select passwords that are unique, ideally random, 16 characters or longer with letters, numbers and punctuation. There are online tools that can help with password generation. • Require password changes at least 6-12 times per year. • Prohibit posting passwords on computers and work spaces. • Provide your team with a multi-user password manager tool if needed.	
Cancel accounts upon employee terminations. Any time an employee leaves the company, either voluntarily or involuntarily, immediately cancel their account.	
Restrict access. Define what data your employees need access to. Restrict access to any area that is not necessary for the job.	
Encrypt confidential information. Use encryption software to protect confidential information on laptops, tablets, backups and other media.	
Reduce spam and phishing vulnerabilities. Scammers use emails that appear to be from legitimate sources to bait unsuspecting users into providing personal information or clicking on links containing malicious software. Ways to reduce these issues: • Adust the protection level of your spam filter to reduce the amount of spam emails that are deposited to inboxes. Employees can assist with this effort by marking messages as spam or forwarding messages to the spam filter, whatever applies. • Train employees how to identify phishing emails, so that they are less likely to click on links to malicious software and provide sensitive personal and company information to scammers. • Have a policy that employees should immediately report any suspicious email that they've responded to or link that they've clicked on, so that you can assess if there are any security concerns.	
Establish two-factor authentication on your web logins and online accounts. This security feature requires two forms of verification to gain access to accounts i.e. a password plus a code that is texted to a smartphone. It stops hackers from gaining access to an account when a password is compromised.	
Perform a secure wipe of all devices and copiers before they are recycled. Often data is retrievable even after it is deleted. A wipe overwrites the info several times making it difficult to recover.	

Limit login attempts on your website. If someone can login to any public part of your website, ensure there is a login limiter i.e. WordPress has a Limit Login Attempts plugin. Hackers use software to attempt thousands to millions of user ids and password combinations to hack a company's website. Utilize software that allows you to set an account lockout threshold. When an IP address fails to input a correct user id and password for a specific number of attempts, the system will lock the user out.	
Adopt a backup plan for your files. The continuity of your business hinges on your resilience in the event of a disaster or your data being compromised by ransomware. Some aspects to consider in your policy: • What storage medium(s) will you use to back up your data i.e. local device or cloud? • How many backups do you need? • How often do you need to back up? Frequency depends on how often you make changes to websites and account data. Ideally, back up your data more frequently than needed. • Where will you store local drives?	
Secure your Wi-Fi networks with encryption and passwords. Securing Wi-Fi networks also means keeping a separate network for guest access, using a different router connection whenever feasible. Change the passwords to Wi-Fi accounts regularly.	
Establish security policies for employees who work remotely. Your level of security may be impacted by an employee's security practices outside of the office. • Work cell phones and laptops must be password protected and never left unattended in public places including vehicles. • Use only a private, secure Wi-Fi and a Virtual Private Network.	
Set firm policies of what apps can be downloaded. Have a policy about what apps employees can install on phones, tablets and computers. • Employees should never jail break their phones or tablets to download apps because this bypasses security features provided by the operating system. • They should be prohibited from downloading applications and visiting websites not related to the job. This will reduce unnecessary risks.	
Consider vulnerabilities related to contractors. Contractor access to your company's network can be a vulnerability if policies aren't in place. If you employ third party contractors who must access your computer network: • Restrict access to only the data that they will need. • Require them to adopt the same security policies as employees where applicable. • When their contract is complete, immediately terminate their user ids and passwords.	
Research local computer support companies who can help. If you get into a bind, you want to have a contact for a trusted specialist who can help you immediately. Establish connections before there are problems.	
Screen companies that you hire to maintain your server. If you hire someone to maintain your server, did you research the best companies and seek referrals from other businesses? How do they protect your data against malware and natural disasters? What are their security policies?	
If a **device is infected** with malware, immediately r**emove it from the network** so that it doesn't affect other computers. Turn off the device and change online and network passwords where possible.	
Be aware of legal requirements for protecting employee and customer data and what to do in the event of a breach. See the State of Oregon Steps for Protecting Data at http://dfr.oregon.gov/business/Pages/protect-data.aspx and Federal Trade Commission at www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.	
Consider taking out a cyber insurance policy that can help defray legal fees and expenses associated with a breach of sensitve employee, customer and company proprietary information.	

City of Portland's Crime Prevention Program: Ask for the Crime Prevention Program Coordinator for your Portland Neighborhood at 503-823-4064 or onicpa@portlandoregon.gov. Visit us at portlandoregon.gov/oni/cp.