

Tips to Protect Your Business From Cybercrime



Sponsored by



Study after study highlights a sad fact. Small businesses are treated as “soft” targets by hackers and cybercriminals.

Consider just a few things that could happen to a small business any day of the week. Phishing emails that try to get employees to give up login credentials. Attempts to break into your databases to steal sensitive customer data. Computers getting infected with malware.

Those of us in small businesses need to be on guard when it comes to cybersecurity.

Luckily, we small business people are getting smarter about how to protect our businesses.

We wanted to tap into that accumulated wisdom of small business owners. So we decided to reach out and ask a group of business people what they have learned and what they advise business people to do for protection.

We asked for practical advice. And we got it!

The following 75+ tips contributed by the Small Business Trends community prove that a little prevention and time spent on basic security, goes a long way toward keeping your business safe.

Are you following the advice in these tips?

Anita Campbell, CEO
[Small Business Trends](#)



TABLE OF CONTENTS



Introduction



Website Security Tips



Finance Security Tips



Back Office Security Tips



Account Management Security Tips

At Microsoft we know that security of your sensitive files and customer data is a top concern.

We also know that many small businesses don't have the resources to put toward the ever-increasing threats of phishing, malware and intrusion attempts. It takes a dedicated 24/7 effort to fight cyber crime.

That's why we at Microsoft have made security a priority.

With our cloud products like Office 365, we offer world class security for your data.

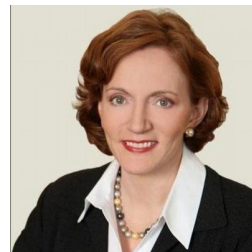
We also dedicate considerable resources to keeping Windows secure as well as devices such as the Surface, Surface Book and Windows phone products. And Azure gives you a secure cloud platform to run your business's proprietary apps.

Of course, even the most secure platform and devices can be defeated by stolen passwords, social engineering tricks and employees clicking on unsafe links. Diligence by individual business users is essential.

That's why these tips, many of them common-sense steps you and your employees can take are important.

For more about security, please also see the Microsoft [collection of security resources](#).

Cindy Bates,
Vice President for US SMB and Distribution at Microsoft



CHAPTER 1

Website Security Tips

Sponsored by



Presented by



Take a Few Minutes to Update Content Management Systems

“Keeping your website content management system updated to the last version will go a long way in reducing the chances of your website getting hacked. Most CMS packages can be updated in minutes and it requires very little skill.”

~ Vedran Tomic of [Local Ants LLC](#)

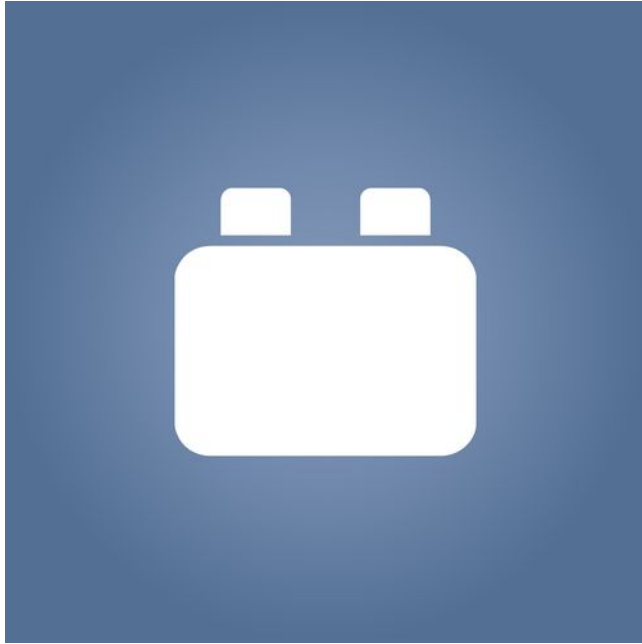


Keep WordPress Up to Date

“The cheapest and easiest step you can take to being secure is to keep your WordPress dashboard updated and use WordPress security plugins. Sadly, this simple step keeps you ahead of the curve.”

~ Amie Marse of [Content Equals Money](#)

Install Good Security Plugins



“Over 100 million sites out there are depending on good ol' WordPress. WordPress is a powerful free tool that can make your website stand out; yet it's also one of the most hacked platforms on the Web.

Install and configure the following plugins to increase your WordPress security:

- Aksimet (to block spam comments).
- Wordfence (to check your site for infection, protect your site from being hacked, and block attacks).
- UpdraftPlus (to schedule backups and make restoration simple, if needed)."

~ Matthew Capala of [Alphametic](#)



Hire a Pro

"This is one of those areas where you should hire a pro. Get your website locked down, get your https set up, make all logins secure, use a password manager, etc - all good things, but threats change and it's great to have someone you trust to make sure you are always up to date and secure in every element of your business."

~ John Jantsch of [Duct Tape Marketing](#)

Use a Security Service to Monitor Your Website

"If using WordPress, regularly back up your database, keep themes, plugins and WordPress up-to-date -- and consider hiring a security service to monitor your install for malicious code. It seems like a pain but it's nowhere near as painful as fixing a hacked server."

~ Robert Brady of [Righteous Marketing](#)



Security Requires Many Steps, Not Just One



"It's not about doing one thing. It's about many basic things, like keeping software and plugins updated, not using the same password everywhere, updating passwords regularly, using two-factor identification when available, blocking 'brute force' attacks by limiting login attempts...

The more obstacles in their way, the more likely a hacker is going to move on to another target, and the less likely their tools (which sniff for known vulnerabilities) will ever bring your site onto their radar in the first place.

That said, keep regular backups going back several months. Just in case."

~ Everett Sizemore of Inflow

Check With Your Web Host Provider for Security Recommendations

“Both your web hosting platform and content management system play an important role in your site's security. You'll want to check with your web host provider about what they do and/or recommend to keep your site secure. If you're using WordPress as a CMS, you'll want to update whenever a new version is released as many updates are designed to fix known security issues. Plugins can also cause security holes, so limit your use of plugins whenever possible, and keep those up to date as well.”

~ Stoney deGeyter of [Pole Position Marketing](#)

Throw this Small Business Myth Out the Window

“The MYTH of the small business: I can do it all. My budget requires me to do it all. At our small business we threw that myth out the window. We work in an environment of abundance. For example, given that security is necessary, we brought on a dedicated expert to keep our data safe. Paul Lowans, our security expert, allows us to sleep well each night. When not checking our systems remotely, Paul communicates with us on new and important plugins and security tools. We recommend you throw the small biz myth out and get a Paul of your own.”

~ Yvonne DiVita of [The Lipsticking Society](#)

Use Strong Passwords for Your CMS

“Today, small businesses need to make sure they have control of their website and its security. Start with strong passwords. Sites using a CMS like WordPress need to be updated frequently, as the software running them is updated often to block hackers. No one wants to wake up to being locked out of their site or, as happened to a client who had ignored updates, find a Viagra ad on their site. Select a website backup hosting option or plugin, and security plugins/programs, so if you do get hacked, you have an easier path back to safety.”

~ Cathy Larkin of [Web Savvy PR](#)



Thoroughly Test Your Backup Procedures

“Make sure your website is protected against hackers -- not just protect the company computers.

Seventy five percent of cyber crimes happen against a small business with the average loss being \$36,000. In addition, thoroughly test your backup procedures if your site is hacked.”

~ Barry Moltz of [Shafran Moltz Group](#)

Migrate Your Website from HTTP to HTTPS



"The most important step small businesses should take to protect themselves from cybercrime is to migrate their websites from http to https. That is fundamental and should not be ignored. Businesses should also train their employees to install firewalls and be wary of which plugins they install, avoiding those that could contain malware.

Besides being prepared for basic cyber attacks (such as DDoS attacks), employees should know how to remove and destroy the hard disks of old computers and devices.

Finally, businesses need to teach their employees to patch all operating systems and applications and to protect their passwords using LastPass."

~ Baruch Labunski of [Rank Secure](#)

Change Your Default Administrative Account ID

“Change the default administrative account ID on your CMS, whether you are using WordPress, Drupal or any other content management system. If potential hackers are forced to figure out both the ID and the password to your site, that's one more obstacle keeping them from compromising your site.”

~ Andrew Schulkind of [Andigo New Media](#)



Get Malware Protection For Your Website

“Protect all of your web sites from malware and hacking. Having virus protection on your computer won't protect your website. Until my site got hacked, I had no idea that they weren't the same thing. Go back to your hosting company, and make sure that you have protection on your site. Don't just opt for the bare bones. Talk to your hosting representative and make sure that you understand exactly what's protected and what the impact is on your site and your customers if you get hacked.”

~ Ivana S Taylor of [DIYMarketers](#)

Register Your Website with an SSL Certificate

“In today's digital age it's more important than ever to keep your website under a virtual lock and key. Make sure your customers feel safe and register your website with an SSL Certificate. SSL Certificates validate your website's identity and encrypt the information visitors send to, or receive from, your site, including sensitive information like names, addresses, passwords and credit card numbers. You can add a certificate yourself, have your web developer help, or call customer support at your hosting or website provider.”

~ Steven Aldrich of [GoDaddy](#)

Install the Wordfence Plugin

“For those running WordPress sites, the best thing you can do to prevent cybercrime is to keep your WordPress installation up to date as well as any plugins you are running. Making sure you are running the most current versions of WordPress and plugins takes advantage of not only the latest features each has to offer but current security patches as well.

Additionally, install and configure the Wordfence Security plugin for WordPress to protect your site against hackers and malware attacks.”

~ David Wallace of [SearchRank](#)

Don't Cheap Out When Going to the Cloud!

“Don't be cheap. Both in terms of what you'll invest as well as how much time you'll invest in picking the right security solutions. Invariably, businesses will choose a cloud-hosting service based on price and convenience, with very little understanding of what they're actually getting. And when it comes to security, not all cloud solutions are the same. The Cloud Security Alliance called out 12 main potential threats in 2016. Do you have the right service provider who can help you mitigate all major risks? Look into that first, before getting lured away by promises of low costs.”

~ Mana Ionescu of [Lightspan Digital](#)

Download Your Backup Files

“Keep your website secure, but also know and plan on the fact that no website is unhackable. Back up your website on a regular basis, and be sure you download the backup files, don't just keep them on the web server. Also have a plan in place in the event that your website does get hacked.”

~ Tim Priebe of [T&S Online Marketing](#)

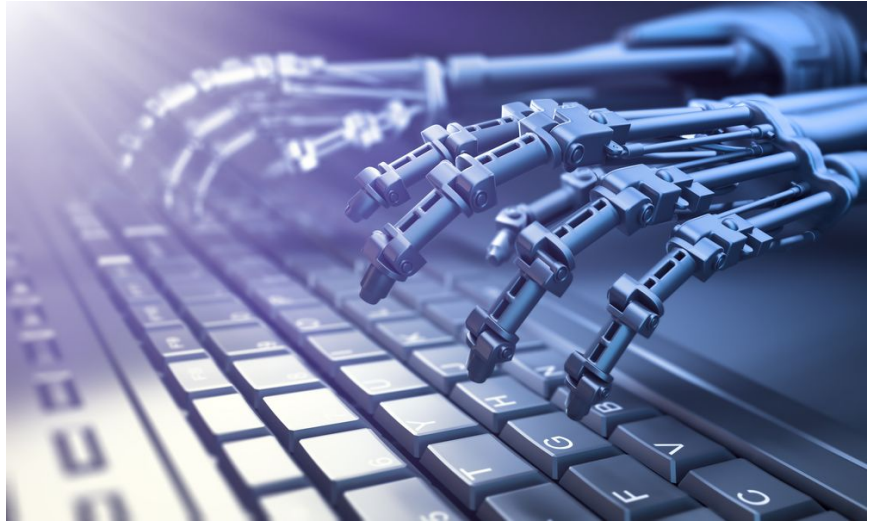
Protect Against the XMLRPC WordPress Exploit

“Protect yourself against the XMLRPC WordPress exploit. A fair majority of Small business websites use WordPress. Most bot attacks are blind and could wreak havoc. A simple fix which could save your business. As perception is reality in the consumer's mind, a compromised website is not acceptable.

Always ensure you have the most recent version of WordPress, and a set schedule to update any plugins.

Monitor your logs for bot attacks and act accordingly.”

~ Daniel Dye of [Native Rank, Inc](#)



Don't Delay Updating if You Want to Stave Off Bot Attacks

"My number one tip for keeping a small business safe from cybercrime is to maintain updates for your software. New vulnerabilities are discovered each day and once a new vulnerability is made public it will be attacked by bots within days if not hours."

~ *Jim Boykin of [Internet Marketing Ninjas](#)*

Use a Hosting Company Obsessed with Security

"When dealing with website hacks one simple change can make a big difference. Pay attention to who's hosting your website. The higher the security on their end, the fewer issues on yours. You need a hosting company that is obsessed with security, so you can focus on something else."

~ *Jamillah Warner of [Gritty Writer](#)*

Use Analytics for Early Warning of Problems

"Many times analytics is used with marketing, but many of the tools were meant to assess website and app performance, which can also aid in preventing hacks. Owners should use a web proxy like Charles or Fiddler to confirm how website or app elements are loaded into the browser. Hack attempts usually impact site or app performance, slowing down elements.

One bonus tip: Keep an analytic report filtered to the IP addresses of store locations and branch offices. Doing so can help sort traffic that is not regular, and highlight traffic from potential fraud sources."

~ Pierre DeBois of [Zimana](#)

Use Automation to Detect Intrusion Attempts

"Use automation to detect intrusion attempts before they occur and harden against them in the future."

~ Emory Rowland of [Leverable SEO](#)

The background of the slide features a close-up, artistic shot of a computer keyboard. Several network ports are visible, with multiple blue Ethernet cables plugged into them. A dense array of fiber optic cables, each with a glowing red tip, extends from the ports, creating a vibrant, multi-colored light effect that fills the upper half of the frame. The overall color palette is dominated by blues, purples, and reds, with a soft, ethereal glow.

CHAPTER 2

Finance Security Tips

Sponsored by



Presented by





Develop a Wire Transfer Approval System

“Implement a rock solid system for making and approving wire transfers, especially large ones, with multiple layers of approvals and protection. Someone recently hacked into our email and sent a message requesting a \$18,000 transfer of our accountant.

Luckily our accountant called my assistant (the one whose account was hacked and supposedly made the request,) and was able to determine that she had made no such request. Since then we instituted a multi-step approval process for any transfers over \$1000.”

~ Michelle Villalobos of [Mivista Consulting, Inc.](#)

Always Log Out of Banking and Finance Websites

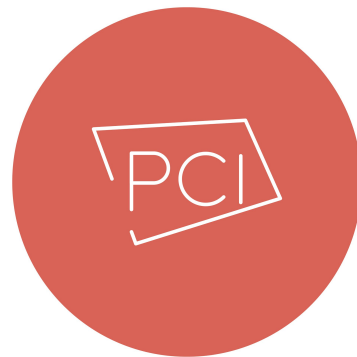
“Small business owners should always manually log out of their banking and money transferring websites, which includes shopping cart services and PayPal. It is also important to avoid using the auto save feature for their username and passwords. Combining these practices with updated security software will help to reduce cybercrime attacks.”

~ Dr. Emad Rahim of [Bellevue University](#)

Make Sure You Are PCI Compliant

“One of the most important items would be PCI Compliance (Payment Card Industry Standard). PCI compliance sets a standard for any organization that collects credit card data. The goal is to ensure the prevention of cyber crimes and identity theft. Most credit card payment gateways enforce this standard, and for good reason.”

~ Seth Rand of [Rand Internet Marketing](#)



Spot Check Your Credit Card Statements Monthly

"It is very easy for bookkeepers and others with company credit cards to steal when paying company bills online.

For example, at an office supply store or a gas station, someone could add their personal purchases to your company's account.

If this person is paying the bills, you, as the owner, will never see it. Make sure you spot check all credit card statements that you pay online at least once per month. And, spot check different credit cards each month."

~ Ruth King of [Profitability Revolution Paradigm](#)



Use a Separate Computer for Financial Transactions



“One of the best tips I've heard for protecting small businesses against cybercrime is to have a separate computer dedicated exclusively to financial transactions.

Don't use this computer for social media, email, games or web-browsing. And of course, make sure the computer is password-protected, and change your password every three to six months.”

~ Ester Venouziou of [LocalShops1 & Live Local! magazine](#)

Use a Banking Platform that Anonymizes Your Bank Information

"Stop sharing your bank account with everyone you do business with. Move to a secure online banking platform that anonymizes your bank information for both vendors and customers."

~ Rene Lacerte of [Bill.com](#)

Guard Against Fake Monetary Requests

"Many security attacks are by external hackers who get employees to unwittingly provide them sensitive company information.

For example, hackers are now breaking into small business servers and hijacking the CEO's email address. Hackers then send a fake email to employees from 'the CEO' asking for bank account and wire transfer information.

Small businesses must set, and continually educate employees in, safe security measures, i.e., immediately inform the CEO of any conversation or email requesting bank, wire or customer data information. Being prepared is being cyber safe."

~ Diane Weklar of [Weklar Business Institute](#)



CHAPTER 3

Back Office Security Tips

Sponsored by



Presented by



Use Email Encryption Tools

“Data breaches occur at large companies almost daily. It’s almost gotten to the point where these breaches have become so commonplace in the news that they don’t even invoke much of a reaction anymore.

The vast majority of data breaches (over 75% by most estimates) occur in smaller businesses.

The biggest piece of advice I would give for small business is to emphasize cybersecurity. Small businesses don’t need to invest tens of thousands of dollars yearly in data security. A relatively nominal investment in the following should go a long way:

- Anti-malware software.
- Email encryption tools.
- Installing consumer grade firewalls.”

~ Ed Hughes of [PrimePay](#)

Unknown Source? Don’t Open Attachments!

“Stop opening attachments from an unknown source and quit visiting suspicious websites.”

~ Laurel Delaney of [Global TradeSource, Ltd.](#)

Do Regular Checks of Your Systems



"The best possible solutions for small businesses against cyber crime are the simplest ones:

1. Be aware of what data you expose.
2. Make SURE that you have a backup in the cloud somewhere for all your data.
3. Use some form of internet security software or service that is designed for small business.
4. Have a protocol in place of what to do if you are hacked so you are not caught without recourse if you are.
5. Do regular "checkups" of your systems (at the very least monthly).

That will take care of 99% of your possible problems."

~ Paul Greenberg of [The 56 Group, LLC](#)

Adopt a Healthy Dose of Skepticism About Emails

"When I worked for an insurance company the secretary Jeanette would block calls from, "The person who really wants to talk to you about an opportunity that can change your life!" But today, small business owners are bombarded with email spam offers that are increasingly deceptive.

Is your business's financial rating in trouble? Does the IRS really need to reach you now? Is that really a message from your credit card company? Spam keeps getting trickier and the best tip is to avoid clicking on or following anything that you can't verify."

~ David Langton of [Langton Cherubino Group](#)

Educate Your Employees

"Educate your employees and team. There's lots of great technology out there to protect businesses but it's the end users who normally create the issues. Educate them so the problems don't come from within your organization."

~ Tom Gazaway of [LenCred](#)

Use Multiple Layers of Security

"It's crucial to have more than one layer of security in place. Having extra layers in place can go a long way in keeping your business safe from hackers and viruses.

And make sure the system you use includes automatic backups of your data...the set and forget type.

You'll sleep better at night. I know I do-because I follow my own suggestions when it comes to combating cybercrime."

~ Joel Libava of [Franchise Selection Specialists Inc.](#)

Develop a Security Breach Management Plan

"Develop and practice a privacy and security breach management plan. Ask to see your vendors' and contractors' privacy and security breach management plan, too.

Prepare for a cybercrime by identifying your risks and mitigate or prevent those risks from happening."

~ Jean L. Eaton of [Information Managers Ltd.](#)

Develop Policies & Procedures



“Small businesses should have policies and procedures that ensure:

- Updated use of malware, spyware and firewall software programs.
- Company, employee and customer data security.
- Enforce their internal security policies.
- Enhance their network, online commerce and banking security.
- Education of email security best practices.
- Password systems.
- Data backups.
- Contingency plans in case of cyber-crime penetration.

All employees should have access to online resources to keep them up-to-date and management should regularly share success stories of cyber-crime prevention.”

~ Franne McNeak of [*Significant Business Results, LLC*](#)

Be Aware of Social Engineering Tactics

"I say put yourselves in the shoes of the cybercriminal. Remember "Catch Me If You Can" which was a movie about Frank Abagnale Jr? He implicitly and overtly used social engineering for his misdeeds. I would offer that an articulate cybercriminal might just do the same by calling into to your switchboard and convincing someone to do a password reset. For example, an estranged husband might call the rural medical clinic to do a password reset on his future ex-wife's patient portal account. Now he's armed with dangerous information for use in stalking and/or divorce proceedings. This is cybercrime!"

~ Harry Brelsford of [SMB Nation](#)

Invest in Security for Employee Devices and Software

"Invest in a full service security suite for your software, intranet and website. Security and backups are everything. Have a strong password policy that changes often. When employees leave, change all passwords that day. Password manager software is an option, but they can be hacked too. Provide secure work laptops for employees. Create security protocols for all employees; review them often. Have a worst case scenario plan in place should you get attacked so things can be set right quickly."

~ Melissa Fach of [SEO Aware](#)

Back Up Data to an External Source -- Automatically



"First and foremost, always back up your data to an external hard drive. Set up times that it happens automatically. To secure your business always read the fine line when downloading information or products. Take note of whom it is coming from and what is attached to it."

~ Patrice Register of [PLR Services](#)

Use a Managed Services Provider

“My advice to a small business owner is to consider outsourcing IT needs to a managed services provider (MSP). For what is generally a very small investment, a MSP can provide SMBs with things like cloud-hosted data storage, state-of-the-art monitoring and security services, and protect both company data and customer data in ways SMBs can't begin to do on a DIY basis. In addition for SMBs for whom compliance is a requirement, a MSP can afford myriad protections related to compliance that are well worth the cost of the service.”

~ Shelly Kramer of [V3 Broadsuite](#)

Train Your Team to Practice “Safe Computing”

“According to a 2014 IBM study, human error factors into 95% of information security and cybercrime incidents. You can protect your company by training your team to practice "safe computing." For example, keep an eye on your mobile devices and laptops so they're not misplaced (even temporarily) or lost.

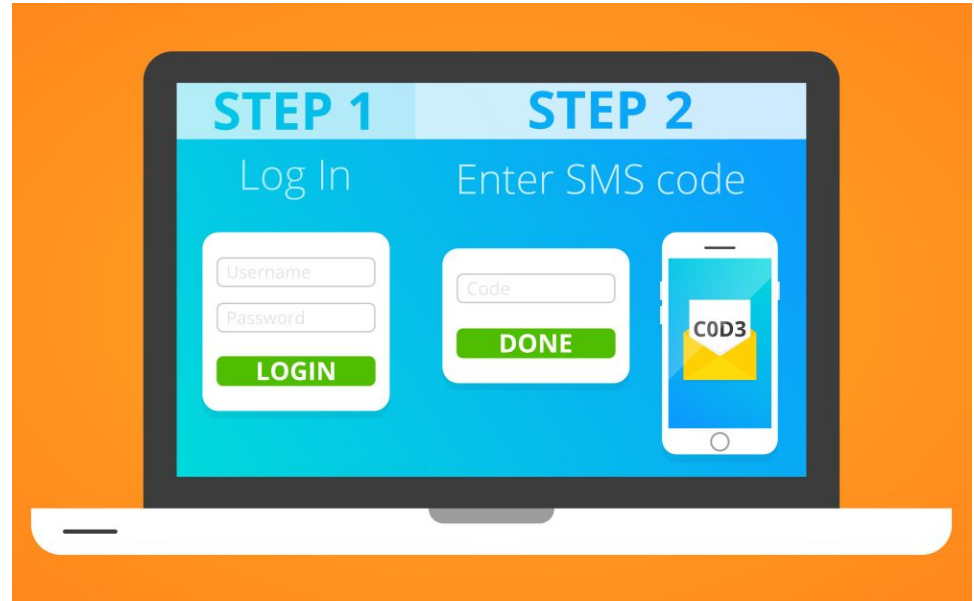
Learn to spot unsafe URLs or attachments so you don't double-click on a bad file. Choose smart/non-obvious passwords, and don't paste them where the whole world can see them. That can go a long way to tightening your security.”

~ Nina L. Kaufman, Esq. of [Ask The Business Lawyer](#)

Use a Two-Step Verification Process

“Explore the two-step verification process for social media sites like LinkedIn, and email services. It could take some time to get used to it, but it is good to be on the safe side. You have to have your mobile phone with you, when you use the two-step verification login process.”

~ *Martin Lindeskog of [Martin.Lindeskog.name](https://www.martindelindeskog.com/)*





Delete Ex-Employee System Access

“Periodically check whom you have given access to your business. Make sure to delete old employees, check everyone's access permissions and send out updated guidelines on what exactly the user should and shouldn't be using their access for.”

~ Cherise Kachelmuss of [Mom and More](#)

Educate Employees To Realize They May Be Targets

“A company's greatest vulnerability is its employees. Hackers will use social engineering tactics to get your employees to unwittingly give them access to your critical data. Teach your people not to click any link in an email, unless they absolutely know who it's from and know the link is legitimately safe. If they click a link that's not legitimate, your company's private data is now vulnerable.”

~ Mike Kappel of [Patriot Software](#)

Conduct Online Searches

“One of the easiest things businesses and brands of all sizes can do to protect themselves from cybercrime, is to take five minutes and do an online search for information and reviews on any new individuals, brands, applications or services they might start using. This simple five minute search on reviews will allow you to quickly know who you are working with. It's one of the absolute best ways to protect yourselves before potentially getting into a nasty situation.”

~ Zac Johnson of [Blogging.org](https://www.blogging.org)

Don't Talk to Strangers!

“Don't talk to strangers! Small business owners receive phone calls, web pop-ups and emails from scammers that often look legitimate. If you get one of these, instead of responding or clicking, take down the information and then hang up the phone or close your browser.

Then, initiate contact on your own with the entity who supposedly sent the information (through your own research on their contact information, not the one provided) to see if it is legitimate. This will prevent you from having your online accounts or computer commandeered by a scammer who looks legitimate, but isn't.”

~ Carol Roth of [CarolRoth.com](https://www.carolroth.com)

Fight Ransom-ware Through Education

“To fight ransom-ware, which is one of the most devastating cyber attack events, train all associates on what ransom-ware is along with the importance of not opening unauthorized unknown attachments. Periodically use an intentional phishing training email - usually from an outside vendor you trust - with a ransom-ware-type attachment to reinforce the importance of defending against ransom-ware.”

~ Kurt Huffman of [Perspectives](#)

Conduct Regular Training to Spot Phishing, Vishing & Impersonation

“Humans (that includes you!) are the weakest link in your cyber security chain. Create a security policy that explains common scams and behaviors employees should avoid to keep your business safe. Conduct regular training in how to spot phishing, vishing and impersonation; the risks of using unsecured networks; and the importance of keeping passwords secret and software updated. Give employees incentives for following the policy -- and negative consequences when they don't.”

~ Rieva Lesonsky of [Small Biz Daily](#)

Never Believe That It Can't Happen to You

"I'll give you a two for the price of one tip. Never think that it can't happen to you, no matter what size your company is. Consult with a professional; as a business owner you can't afford to try to keep up with all the changing ways cyber villains can attack you. It's worth the investment -- to you and your clients."

~ Will Moreland of [Will Moreland International, LLC](#)

Be Proactive About Security

"Make sure all employees have awareness of cybercrime and learn how they can detect and prevent it proactively."

~ Harry Vaishnav of [Small Biz Viewpoints](#)



Beware of Attempts to Exploit Human Ignorance

“Train your team on how to identify and defend against common social engineering hacks. These incredibly effective “hacks” □ aren't even hacks at all, in a strict technical sense, since they're not attempting to bypass safeguards on your IT systems. Instead, they attempt to exploit human ignorance.

You don't need to break the lock if you can trick someone into handing you the keys. If your team is not aware of the common social engineering techniques out there, they may end up handing over the keys to the castle without even knowing it.”

~ Justin Hughes of [RealtyMogul.com](https://www.realtymogul.com)

Plan for Mobile Device Security

“Every business should provide instructions for dealing with security on mobile devices of all types. Security plans should include how to report lost assets. Devices should have software applications installed to ensure they are completely protected. Tablets, smartphones and laptops should have the same level of antivirus, firewall, and security protections desktop computers have.

Mobile devices can be disabled or even have the data erased remotely as the ultimate protection against theft or data loss. Android, iPhone and Windows all provide the ability to completely erase your data.”

~ Gail Gardner of [GrowMap](https://www.growmap.com)

Conduct Internal Audits

"Small businesses should conduct an internal audit to identify the most critical data, and then apply the bulk of their budget and resources to protect the "crown jewels" with more stringent controls.

Because user convenience trumps security [when it comes to employee behavior] look for automated, policy-based solutions, which offer a multilayered approach to secure devices, data and the corporate network -- and makes it easier to enforce policies, protect assets and block malware."

~ Laurie McCabe of [SMB Group](#)

Always Use "Genuine" Software

"My advice would be to use genuine products. Always avoid using those fake or 'nulled' ones as they can do more harm than good.

Spending a little more will always save you more money in the long run!"

~ Reginald Chan of [Reginald Chan](#)

Have a Good Legal Plan and Security Policy for Employee Termination

"In addition to a good legal plan for an employee termination, implement these security policies for terminated employees:

- Promptly change passwords for employees' system access and cloud based products (e.g., document management).
- Evaluate risk that an ex-employee can access a company system through a current employee's account.
- Preserve emails before deleting the account; assign the user email to someone for monitoring.

Law firms are at special risk - make sure the ex-employee no longer has access to your online legal research tools or court filing systems (Pacer), or can change your litigation deadlines (prevent malpractice)."

~ John Browning of [Browning Law Group](#)



Provide Training on How to Spot Phishing Attempts


“As a business owner, it is critical to understand the primary reason businesses get hacked is because an employee is tricked into opening a phishing email. Security Awareness Training educates employees how to spot a phishing attempt, greatly reducing the odds that they can be fooled into opening or downloading something they shouldn't.”

~ John French of [RESULTS Technology](#)

Create an Internet Usage Policy

“Take a strategic approach with a company policy regarding use of the Internet and online companies. Recent research by Gallup shows that the Millennial generation has the most 'trust' in online businesses and institutions. This likely comes from the fact that they have spent most of their lives connected to the Internet through smartphones, laptops, tablets and wearable technology. They don't know anything different. 'Trust' or 'don't trust' has little meaning for them, but they do matter to any small business owner. Let them know early on what they can or cannot do online via company computers. Protect your firm!”

~ Terri L Maurer of [Maurer Consulting Group](#)



CHAPTER 4

Account Management Security Tips

Sponsored by



Presented by



Remind Employees Often of Security Measures

“One thing small business owners can do now to protect their businesses from cybercrime is to educate employees on basic security measures in the office. Our employees are our biggest defense against cybercrime but also our biggest weakness. Remind them often on basic steps - update passwords, backup files to a protected space, keep an eye out for any type of potential threat and report it immediately, etc. The more you educate your team, the better chance of ensuring safety against cybercrime at the office.”

~ Nellie Akalp of [CorpNet.com](https://corpnet.com)



Separate Wi-Fi Connections

“If you have a Wi-Fi connection, separate it into 2 connections rather than one. One for business and one for guests. This also allows control over both, but limits who can access either one. First, have the Business Wi-Fi set to a “Super Secret Password” □ that only computers belonging to the network/domain will have access to the password, whereas the guest Wi-Fi password would be available on request, but have no access to network resources, only have access to the internet, and is monitored for Viruses, Spam Email, and Content Filtering, using a Unified Threat Management Gateway (Firewall).”

~ Laura Bennett of [Embrace Pet Insurance](https://embracepetinsurance.com)



Use Complex Passwords

"Educate yourself and employees to be security aware. Use complex passwords, change passwords, be less trusting, don't write passwords down, be leery of public (free) WiFi, treat security seriously, think before you click on web site links. While backup, security software and a properly configured network is important - those things will be of no value if you allow a hacker to access your networking using your security information."

~ Ramon Ray of [Smart Hustle Magazine](#)

Enable Password Protection on all Mobile Devices

"Be sure all your mobile devices (cellphones, tablets, laptops) have password protection so your information won't be compromised if a device is lost or stolen."

~ Barbara Weltman of [Big Ideas for Small Business, Inc.](#)

Enable Two-Factor Authentication

"Based on what I see talking to a lot of new founders, it's not the advanced hackers that cause most of their security headaches; it's simply sloppy mistakes like using obvious passwords and forgetting to back up important files. Do the simple things right -- choose hard-to-crack passwords, back up everything, use secure tools and set up two-factor authentication for apps where it's available -- and you'll be more protected than most."

~ Alex Turnbull of [Groove](#)

Thoroughly Vet Marketing Partners

"Since hackers often gain access to systems via compromised accounts, a key to protecting yourself is to help protect your customers. From a marketing perspective, this means adhering to a strict brand image in all of your marketing and communications, and protecting data through advanced passwords and technologies."

Further, thoroughly vet your marketing partners. There are services available to marketers that are extremely valuable, and require a code snippet to be added to your site. Review the code and security precautions before adding any code to your site, as they could also be a potential point of entry."

~ Sarah Bundy of [All Inclusive Marketing](#)

Keep a Vault of Passwords

“The mysterious password.... Make all of your passwords really complicated. It’s too easy to make our passwords relevant and easy to remember. We want to be able to remember them in the moment. You’re better off making them complicated and impossible (or really hard) to remember. The less relevant they are, the harder they are to figure out. And you can always keep a vault of passwords so you, and you alone, have access to them. Keep your passwords a mystery – even to you. You’ll keep your business safe.”

~ Diane Helbig of [Seize This Day](#)



Avoid the Use of “Master” User Accounts

“Small business owners should avoid creating any type of “master” user account and password where an employee or individual can gain access to all the company’s financial information. To be proactive consider subscribing to a business credit monitoring service which gives access to your business credit report 24/7. Take advantage of email alert notifications so you can be notified of any new activity occurring on your company credit files in real time.”

~ Marco Carbajo of [Business Credit Insiders Circle](#)

Use a Password Manager

“In a small business there is a need for several employees to share an account login for a website or other internet cloud software. Using a Password Manager you can keep the information secure and controlled and at the same time allow easy access to employees who have to use these accounts.

If you use LastPass you can share the credentials without sharing the passwords. Look for security features like the Facebook Business Manager where you can share access to the business pages without sharing the passwords. If the software offers email alerts or 2 factor authorization. Use it.”

~ Shashi Bellamkonda of [Surefire Social](#)

Make Security a Priority Internally

“Regardless of the size of your business, security needs to be a priority. At Nextiva, we try to keep a variety of passwords dedicated to different accounts and devices, and change those passwords frequently. With that extra layer of security, we feel much more protected from the threats of cybercrime.”

~ Yaniv Masjedi of [Nextiva](#)

Develop a Secure Onboarding/Offboarding Employee Process

“Make sure you have a secure process for onboarding new employees with passwords and access to company records, and off boarding employees who are no longer with the firm. Many companies are lax about how and when they remove passwords and access for former employees. The day an employee leaves your company for any reason is the day all of their passwords should be changed. Do a periodic audit to make sure this is happening, especially if your company is expanding to new markets and new geographies.”

~ Dawn Fotopulos of DF Consulting, Inc.

Make Sure You Keep Everything Patched!

“Don't use obvious passwords (e.g. 123456, password, football) and, additionally, consider using a password manager which keeps track of your passwords, generates new passwords, and it's a great way to share accounts across a company.

Make sure that you keep everything patched (and that includes hardware like routers!).”

~ Matt Mullarkey-Toner of [GetApp](#)

Implement a “No Duplicate Passwords” Policy

“Implement a password policy. The policy would promote best practice and improve security. It can cover things like, - how often employees change their password - what passwords should consist of to make them more complex (i.e. one upper case and one number) - and mandate that the same password can not be used for different accounts. This is a simple, but critical step to protect your business.”

~ Brenda S. Stoltz of [Ariad Partners, LLC](#)

Don't Re-Purpose Old Passwords

"Don't re-use passwords from one account to another. If any one of them gets hacked, if you re-used the same username and password on other services, those will be vulnerable, too."

~ Larry Kim of [WordStream, Inc.](#)



Enable Login Notifications

"Teaching basic password security throughout the organization is a great place to start, but it is not the only thing to be concerned about."

If you have employees who have access to important company assets, then make sure they have things like login notifications, 2-factor authentication, and other security measures setup.

That way, if someone does try to log in to their company accounts, they will be notified immediately and it hopefully won't do any damage to the company."

~ Kristi Hines of [Kristi Hines Media LLC](#)



Make a List of Online Assets

"I make sure all my clients have a complete list of online assets including website information (where it is hosted, registration information, etc.), all social media administrators, logins and passwords, and other place listings for the business online (such as Yelp). This list should be kept offline in a safe place with access by at least two individuals."

~ Marsha Pearson of [Email Marketing Guru](#)

Update Passwords At Least Every 6 Months

"One of the things small businesses get a bit complacent on is changing passwords every 6-12 months. Sophisticated cyber criminals have a much higher chance of hacking accounts when passwords don't change. Update your browser software to the most current versions and regularly change your passwords. Create a document for all your sites and their passwords and store it in a safe place both online and printed out."

~ Deborah Shane of [DeborahShane.com](#)

Invest in Secure Access Tools

“The majority of breaches today are a result of compromised administrative credentials. Hackers often target free and legacy access tools as an entry point because of the known lack of security. Invest in secure access tools to manage remote access to your network.

While small businesses may have trouble justifying the upfront cost of a paid tool, it pales in comparison to the financial fallout of a breach. Couple a secure tool along with unique passwords and two factor authentication, and greatly mitigate the risk of cybercrime.”

~ Sam Elliot of [Bomgar](#)

Use Devices with Fingerprint, Voice and Facial Recognition Features

“Using a service like LastPass for password management can help. And look for devices that use biometric products and services like fingerprint recognition, voice recognition and facial recognition to safeguard devices and make it harder for people to access your information.”

~ Brent Leary of [CRM Essentials](#)

Adopt a Hybrid Cloud Strategy

“First and foremost, small business owners need to be aware that cybercrime is real, and then start to focus on preventive actions in response to it - e.g., better password management, adopting a hybrid cloud strategy, and raising company-wide awareness of the potential problems. Small businesses make great cyber attack targets because the owners think cyber attacks only happen to big companies. The truth is far from it.”

~ *Ivan Widjaya* of [Noobpreneur](#)

Don't Store Proprietary Materials Online

“Protecting your business from cyber bad guys is akin to being on a diet. If you want to lose weight don't eat foods that make you fat. Same theory for online security; if you don't want to be visited by cyber-crooks, don't store sensitive or proprietary materials online.

Criminals can grab your info from third parties even without your help, but it's best to always be as proactive as possible. Use the cloud and separate hard drives. Change passwords and don't use the same one for all.”

~ *Gayl Murphy* of [InterviewTactics.com](#)

Train Your Employees to Better Prevent Cyber Crime

“Encourage your staff to use smarter passwords - change them often and never use the same one across multiple platforms. Passwords should never be stored in the cloud or on a sticky note in the office.

Red flags employees should watch for include emails that ask for credit card or other personal information, requests for immediate action regarding unfamiliar situations, and emails with suspicious attachments. Never forward or reply to a suspicious email, and inform the email service provider by reporting the email as spam.”

~ Megan Totka of [ChamberofCommerce.com](https://www.chamberofcommerce.com)

Email is the Key to Everything - Secure It

“The best way to keep your business safe from hackers and cybercrime is to be proactive. For example, make sure you have a different password for your email than anything else. And change it periodically. Email is where password reset links and codes are sent, so if a hacker initiates a request on one of your other accounts, make sure they can't get into your email.”

~ Laura Rubinstein of [Transform Today](https://www.transformtoday.com)

Ensure Your Username is Different From File Access Names

"First, my doctoral thesis is on white-collar crime, and I assisted the SEC in taking down white-collar crime in Los Angeles. (Intentionally vague to protect the innocent.)

Using the 'cloud' is something that truly improves efficiency and productivity. However, there is no such thing as assumption of security, even in the cloud.

Tip: If you have a file allowing for password protection, enable that password protection. Then, ensure that the actual username is different from what is presented with the file access. In other words ... misleading the hacker."

~ Deborah Anderson of [Tech Audit](#)



Use Complex Autogenerated Passwords

“Something as simple as integrating a password manager/vault solution is an inexpensive but powerful way small businesses can protect their applications and data. Not only do password manager solutions help businesses keep track of passwords for all software applications and online accounts, but they can also automatically generate more complex passwords for new accounts that are harder to crack/hack.”

~ Terrance Gaines of [Terrance Gaines Tech](#)

Make Sure Privacy Settings are Adjusted on Social Media Accounts

“Implement a social-media policy for the company's social media accounts. The policy should provide guidelines around what can be disclosed about the company and who is allowed to speak for the company. Make sure the privacy settings are adjusted properly on all accounts to protect against hacking.”

~ Andre Ankton of [Innovarus Marketing](#)

Many Thanks to All Who Contributed!

The information in this ebook is provided by the individual contributors identified. The presentation of this ebook as a whole is the copyright of [Small Business Trends](#), LLC, 2016. Many thanks to Microsoft whose underwriting support made the collection and presentation of this ebook possible.

Image credits:

The Microsoft logo and the Small Business Trends logos are owned by the respective companies.

The following images in this ebook are through license with Shutterstock:

[Lock](#), [Digital Background](#), [Laptop](#), [Plugin](#), [Lock](#), [Key](#), [Password Security](#), [Malware](#), [Backup](#), [HTTPS](#), [Bot](#), [Network Cables](#), [Approved](#), [PCI](#), [Credit Card](#), [Double Computers](#), [Keyboard](#), [Hacker](#), [Policies](#), [Hard Drive](#), [Google Authentication](#), [Ex-employee](#), [Proactive](#), [Ex-employees](#), [Network Cable](#), [WiFi](#), [Password](#), [Vault](#), [Login](#), [Checklist](#), [Access](#)