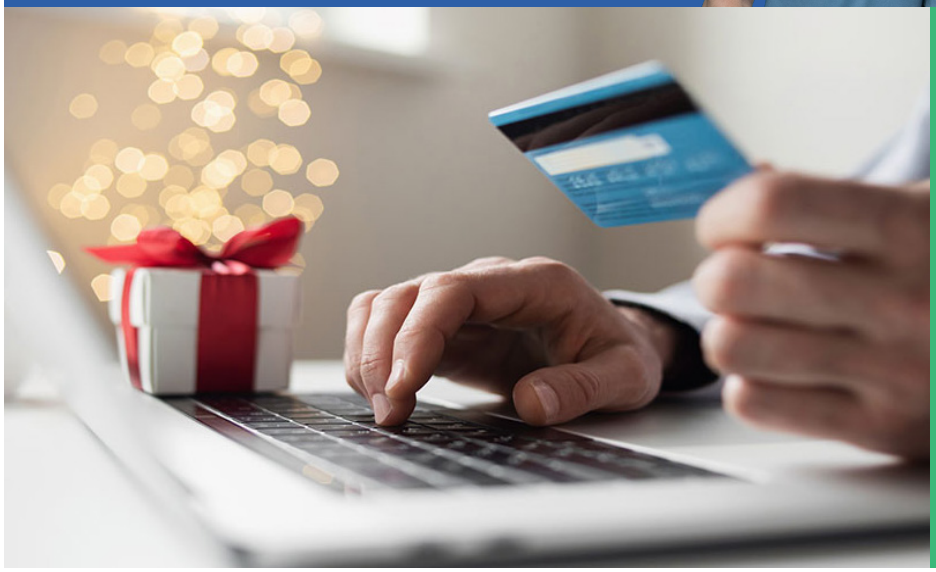
Cybersecurity Source

Cybersecurity and Technology Tips To Help Your Business Run More Securely, Efficiently and Profitably



Business leaders depend on their IT systems. SimplifIT allows you to focus on growing your business with secure and compliant IT solutions that are proven to work & keep you safe.

- Craig Willard, COO
- Eric Elder, CTO
- Nick Landers, CMO

SimplifIT MANAGED IT|CYBERSECURITY

DON'T LET HACKERS RUIN YOUR HOLIDAYS

The holiday season has arrived, and more Americans are expected to turn to online shopping this year than ever before. The ongoing pandemic, combined with convenience, makes online shopping an obvious choice for most consumers.

Unfortunately, online shopping has been muddied with hackers and cyberthieves since its debut. There are still safe places on the Internet where we should feel comfortable to shop, though. If you are careful about where you spend your money or share your personal information, online shopping can feel just as safe as entering a store.

CONTINUED ON PAGE 2

Inside This Issue

CONTINUED FROM COVER

Here are our five best tips to ensure that your online holiday shopping is safe and secure.

Stick To Secure Websites

When shopping online, you want to ensure that every site you visit is secure. Look at the browser bar when entering a new site. If there is a small padlock icon to the left of the web address, the site is secure and you should feel safe to continue. Google Chrome goes an extra step and will label unsecure sites as "not secure" so you know to stay away. Another quick way to tell if a site is secure is by looking at the web address. If it begins in "https," you're good to go. If the "s" is missing at the end and it starts with "http," the site is not secure, and you should find somewhere else to shop.

Don't Be Afraid To Use Your Phone

You can shop on your phone just as easily as you do on your computer, and the portable aspect should not worry you. Major corporations like Amazon and Walmart have secure apps with seemingly unlimited items to purchase. Making purchases directly on apps avoids the hassle of going to the company's website, where your connection might not be as secure. It also helps to set up an Apple or Google Pay account, as businesses will not be able to get your bank account information from these sources.

If you do decide to shop on your mobile device, make sure that you are not on public WiFi. Public WiFi is rarely secure, and using it could make you an easy target for hackers. They could get any personal information you enter while on the WiFi. It's better to bookmark the products and purchase them when you are on a private connection.

Use A Password Manager

To keep your information secure, it's imperative to utilize strong and complex passwords that are difficult to crack. Avoid using personal information and using the same password across accounts. To make things easier for yourself, utilize a password manager to keep track of all of your different passwords. This way, you can create complex passwords that even the best of hackers can't figure out. Make sure to use a mix of uppercase and lowercase letters, numbers and special punctuation to make the most secure password possible.

Take A Pass On Amazing Deals

If you come across a price that just seems too good to be true, chances are it probably is. If you search for an item on a search engine, you may see prices way lower than those of major retailers. These options could be on unsecured sites as a front to try to steal your information or it could be someone who doesn't actually have the item trying to make a quick dollar. While the deal might seem like something you can't pass up, it may cost you more in the long run, and you might not even get the product.

Pay Attention To Bank Statements

You won't always know when someone gets access to your personal information or bank accounts. By paying attention to your bank statements, you can catch overcharges or purchases that you did not make. Always use a credit card when shopping online because hackers will not be able to access any of your actual money. Most credit cards come with fraud protection that prevents you from being liable for charges you never actually made.

As long as you take the necessary precautions, shopping online is a safe and financially responsible practice. If you follow these tips, your holiday shopping will go as smoothly as possible.

SimplifIT News

Merry Christmas & Happy New Year

At this season, we want to say thank you to our clients and newsletter subscribers. You are some of the most business-savvy individuals we know. We love watching you grow your business, and we learn much from your commitment to YOUR clients, and your true understanding of service. We appreciate your desire to learn and hope this newsletter will help you be a better leader, manager and business professional.

As we wrap up this year and look forward to 2022, we wish you, your team and your family a Merry Christmas and Happy New Year!

Trivia

Who wants to win a $25 gift card?

You can be the winner of this month's trivia challenge. Just be the first person to correctly answer this month's trivia question and receive a $25 Amazon gift card!

What is the highest grossing Christmas movie of all time?

A. The Santa Claus
B. Home Alone
C. Home Alone 2
D. Elf

Ready? Call us right now with your answer!
502.783.6630

The Easiest Way To DISASTER-PROOF Your Cybersecurity

Though no one would dispute the increasing prevalence of cyber-attacks on businesses in recent years, many small-business owners believe themselves and their business to be immune to such attacks. Broadly speaking, many small-business owners are likely to think that cybercriminals will go after the bigger fish.

The fact of the matter is that cyber-attacks are crimes of opportunity, and small businesses often have access to a good amount of sensitive data without many major safeguards. In other words, they're low-hanging fruit, ripe for the picking.

Back in 2019, two-thirds of respondents to a survey about cyber security didn't believe that their small to mid-size business (SMB) would fall victim to a cyber-attack. Consequently, only 9% of respondents said cyber security was a top priority for their business, and 60% didn't have any sort of plan for deterring a cyber-attack. All of this, despite the fact that, according to a recent report from CNBC, SMBs endured 43% of reported cyber-attacks, and according to data from the Ponemon Institute and Keeper Security, 76% of SMBs in the U.S. alone reportedly endured a cyber-attack within the previous year.

Every small-business owner should have some plan for deterring cyber-attacks so they don't end up as another statistic. Here are a few strategies for keeping the cybercriminals at bay.

Boost Your Cloud Security

Storing data in the cloud is easy and cost-effective, but you should take care to find the most secure cloud storage platforms. Not all cloud platforms make security a priority, but some do.

Secure All Parts Of Your Network

Our computers and the many smart devices hooked up to our network can become weak spots for hackers to get in. Taking steps to safeguard each device in your network with strong passwords and robust authentication measures will go a long way toward keeping the hackers at bay. In fact, one of the most basic security measures you can take for your network is to restrict access to your WiFi with a strong password.

Invest In Extra Security Measures

Virtual private networks (VPNs) and firewalls are tools that are highly effective in protecting against cyber-attacks, even if they can't prevent 100% of them.

Pay Attention To Updates & Upgrades

When you get notified that one of the technological tools that you use has a new update, it's easy to ignore it. However, you should commit to regularly updating and upgrading these tools because developers will often add patches to their programs that make them more secure against attacks with each update. So, it behooves business owners to regularly install updates for their tech tools.

Back Up Your Data

With one of the most common forms of cyber-attacks being ransomware attacks, where hackers will hold your company data hostage until you pay them a ransom amount, having your company data stored on multiple backups can ensure that your business won't crumble due to your data's inaccessibility.

Limit Employee Access To Your Network

As much as we'd wish it were true, many cyber-attacks don't come from outside of your company. Instead, they originate from within. If you want to limit the amount of damage that someone inside your company can do in a cyber-attack, the best course of action is to limit their access to different parts of your network.

Train Your Employees

At the same time, just as many cyber-attacks occur not because of an employee's malicious intent, but because of their ignorance. They click on a link in a sketchy e-mail and fall for a phishing scheme, volunteer their password info without thinking about it or choose a weak password for their computer. That's why you need to dedicate time to training your employees on best practices when it comes to security.

Set Up A 'Security Culture' At Your Workplace

You need to make cyber security a top priority, not just for your IT department, but for every department at your business. When everyone works together to protect their workplace from a cyber-attack, you have a better chance of actually succeeding.

Will protecting your business from a cyber-attack require a good amount of time and money? Absolutely. Can you afford to ignore the prevalence of cyber-attacks any longer? Statistically, no. The sad truth is that 60% of SMBs that fall victim to a cyber-attack end up shuttering within six months. Don't put yourself in that kind of position. Instead, take your business's cyber security seriously.

Simplif IT
MANAGED IT | CYBERSECURITY

112 East Main Street
Frankfort, KY 40601

502.783.6630

WeSimplifIT.com

THE DIGITAL-FIRST ECONOMY

Whether your business is a massive multinational operation or you're a humble "solopreneur," you have now entered the era of the "digital-first" economy. Daunting though it may be to prioritize your business's online presence, there are five traits that will serve your customers well and lead to your success.

Flexibility: Be prepared to constantly advance your knowledge of new technologies and softwares and make changes to your systems when necessary.

Comfort With Outsourcing And Automating: Don't be afraid to delegate tasks, such as fulfillment or marketing management, that keep you from the core work of your business.

Digital Communication Skills: This means not only having the right kinds of digital communication avenues (e-mail, website, social media, etc.) but also knowing how to optimize them to communicate clearly and consistently with your customers.

Understanding Customer Expectations: In a world where customers expect seamless interactions and quick results, make sure you each clearly understand one another's needs.

Cyber Security: Even solopreneurs are at a greater risk for cyber-attacks. Make sure to protect sensitive data in a way that works best for your business model.

HOW TO MAKE YOUR PHONE MORE SECURE IN LESS THAN 1 MINUTE

If you want to protect your smartphone from being hacked, all you have to do is turn your phone off and back on again. Does that sound overly simplistic and cliché? Probably. Does it work? Absolutely.

The reason that simply turning your phone off and on again can thwart hackers is because, historically, hacking has been a game of persistence. Keep at it for long enough, and a person's security protocols will eventually give.

However, with smartphones, hackers have found that they don't need to be persistent because most of us never shut off our devices. Thus, hacking smartphones has become a much more attractive option for cybercriminals.

By simply turning your phone off and back on again regularly, you give cybercriminals far fewer opportunities to hack your device, and they'll likely move on to try and hack a smartphone that stays on continually.

With this easy, low-tech solution, there's no reason that anyone with a smartphone shouldn't be doing it.

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now!

At no cost or obligation, our highly skilled team of IT pros will conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.

The assessment can be conducted 100% remotely, with or without your current IT department or provider, and is free of charge or obligation. With only 60 minutes of your time, you can be on your way to plugging these critical GAPS that could be costing you THOUSANDS.

To get started and claim your free assessment now, **call our office at (502) 783-6630.**