STRONGHOLD SERVICES
Business I.T. Specialists

Technology Times

"Insider Tips to Make Your Business Run Faster, Easier and More Profitably"

Did you Know

With the rise of eCommerce and online banking, cybercrime has evolved. Like criminals who pull smash-and-grab jobs, they go where the money is. However, unlike bank robbers, cybercriminals do their best to avoid detection by letting malware do the work for them. Viruses and ransomware sneak into PCs to quietly steal passwords, financial credentials, and other personal information to be sold on the black market for profit. Not all malware is stealthy though. Here are some telltale signs.

- Slow computer
- Blue Screen of Death (BSOD)
- Lack of Storage Space
- Suspicious Modem and Hard Drive Activity
- Pop-Ups, Websites, Toolbars, and Other Unwanted Programs
- You're Sending Spam

It's always smart to perform regular malware scans to ensure your business is safe. To find out more about malware and IT security, contact us today. (519) 471-9999

March 2020

This monthly publication is provided courtesy of Stronghold Services Corporation.

Our Mission:
To create and build professional, valuable and exceptional relationships with our clients; to develop and implement the most appropriate and effective technology solutions and processes.

Clear Signs You're About To Get Hacked … And What To Do NOW To Prevent It

Do you use the same password for everything? If you do, you're not alone. We all have bad cyber-habits, whether it's reusing passwords or connecting to unsecured WiFi. These habits can make it easy for hackers to steal our personal information and use it for their own purposes – or they can sell it on the dark web for an easy profit.

These are habits you have to stop right now – and habits your employees need to stop too. After all, good cyber security practices are a group effort! But using the same password for everything or using simple passwords aren't the only things that are going to get you into trouble. Here are three more clear signs you're setting yourself up for a breach.

Sharing Your E-mail

Countless websites want your e-mail address. Sometimes it's not a big deal if you're sharing it with a vendor or e-commerce site. You want to ensure you receive invoices and shipping confirmation. But other websites just want you to sign up for special offers, notifications, e-mail newsletters and other inbox clutter. It sounds mostly harmless, but what they fail to tell you is the fact that they're going to sell your e-mail address to advertisers and other third parties.

To make matters worse, you have no idea where your e-mail address will end up – or if it will fall into the wrong hands. Hackers are constantly on the lookout for e-mail addresses they can take advantage of. They use e-mail for several different kinds of cyberscams – most notably phishing scams. Hackers can even make it look like an e-mail is

Continued on pg.2

Continued from pg.1

coming from a legitimate source to get you to open it.

Whenever possible, avoid using your work or personal e-mail. If you need to sign up for something and you don't completely trust the source (or just want to avoid spam), create a "burner"
e-mail address you can use. It should be something different from your work or personal e-mail and not associated with business or banking.

Not Using HTTPS

Most of us are familiar with HTTP. It's short for Hypertext Transfer Protocol and is a part of every web address. These days, however, many websites are using HTTPS – the S standing for "secure." Some web browsers, like Google Chrome, even open HTTPS websites automatically, giving you a more secure connection. Of course, this only works if the website was made with an HTTPS option.

Why is visiting an unsecured HTTP website dangerous? Any data you share with an unsecured website, such as date of birth, passwords or any financial information, may not be securely stored. You have no way of knowing that your private data won't end up in the hands of a third party, whether that's an advertiser or a hacker. It isn't worth the risk.

When visiting any website, look in the address bar. There should be a little padlock. If the padlock is closed or green, you are on a secure website. If it's open or red, the website is not secure. You can also click the padlock to verify the website's security credentials. It's best practice to *immediately* leave any website that is not secured. And never share your personal information on a web page that is not secure.

Saving Your Passwords In Your Web Browser

Web browsers make life so easy. You can save your favourite websites at the click of a button. You can customize them to your needs using extensions and add-ons. And you can save all your usernames and passwords in one place! But as convenient as it is, saving passwords in your browser comes with a price: low security.

If a hacker gets into your saved passwords, it's like opening a treasure chest full of gold. They have everything they could ever want. Sure, web browsers require a password or PIN to see saved passwords, but a skilled hacker can force their way past this hurdle if given the chance.

Use a password manager instead. These apps keep all of your passwords in one place, but they come with serious security. Even better, many password managers are designed to suggest new passwords to you when it's time to update your old passwords. LastPass, 1Password and Keeper Security Password Manager are all good options. Find one that suits your needs and the needs of your business.

> **"Many password managers are designed to suggest new passwords to you when it's time to update your old passwords."**

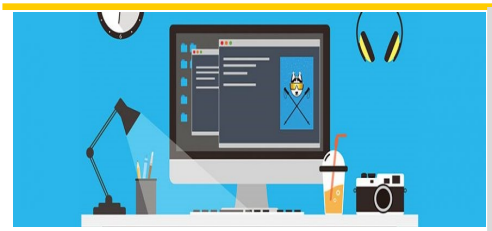
Office 365 hacking: What you need to know

Some hackers have become so skilled that they don't even need you to give up your credentials to hack into your account. One recent cyberthreat is targeted towards users of Microsoft Office 365. You don't want to be the next victim, so read up.
https://www.strongholdservices.ca/2020/01/22/office-365

A phishing scam that harvests users' credentials

The latest cyberattack on Microsoft Office 365 involves harvesting users' credentials. Scammers use this previously unseen tactic by launching a phishing message to users, asking them to click on an embedded link. What makes this scam more insidious than traditional phishing scams is that the URL within the message links to a real Microsoft login page.

Successful attacks could result in an unimaginable catastrophe to your company. For tips on how to spot this and other nefarious scams and how to plan thorough security practices, contact our experts today.



Add hours to your day with these PC hacks

Because there are only so many hours in a workday, it's vital to make the most of your time. If distracting websites, unorganized files, and cluttered inboxes prevent you from getting work done, consider these tips to better manage your time and stay productive at work.

Get rid of clutter

You can also decrease distractions and increase your output by deleting old files, uninstalling unused programs, and organizing documents into appropriately labeled folders. This makes finding files easier and improves your computer's performance as well.

Block sites that waste your time

Visiting non-work-related websites hinders productivity. A quick five-minute break to check your Facebook feed may not seem like much, but a few of those per day add up to a lot of time.

If you and your employees have trouble staying away from social media sites like Facebook, Instagram, and Twitter, it's a good idea to block access to them using URL filters

Use keyboard shortcuts

Mastering keyboard shortcuts will make it easier and faster to perform simple functions. There are more than a hundred useful shortcuts, but here are the most common shortcuts you should keep in mind:

- **Ctrl + C, Ctrl + V, Ctrl + X** – to copy, paste, and cut selected items
- **Ctrl + Z** – to undo an action
- **Alt + Tab** – to switch between open apps
- **Alt + F4** – to close the active app

For more of these, take a look at this updated list of advanced shortcuts for Windows.

https://support.microsoft.com/en-ph/help/12445/windows-keyboard-shortcuts

Are You Working SMART?

Rubbermaid thought they needed more products to be the leader in their industry. So, they set out to invent a new product every day for several years, while also entering a new product category every 12-18 months. *Fortune* magazine wrote that Rubbermaid was more innovative than 3M, Intel and Apple; now, that is impressive.

Then Rubbermaid started choking on over 1,000 new products in less than 36 months. Innovation became more important than controlling costs, filling orders on time or customer service. They ended up closing nine plants and laid off over 1,100 employees before Newell Corporation came in to buy (rescue) the company.

I had a mentor who once told me, "Rob, I don't care how hard you work. I care how smart you work." Rubbermaid was working hard, putting in time, money and effort while at the same time destroying their own company. How did that work out for them?

Eli Lilly thought they needed to hire 2,000 PhD researchers to create more products to keep Wall Street happy with their growth. The only problem was they didn't have the funds to hire them. So, they had to come up with another way to solve this problem – in other words, they had to work smarter.

They decided to take all their molecular problems, post them on the Internet and tell all molecular PhD researchers that they would PAY for solutions. Instead of having to pay the salaries and benefits for 2,000 new researchers with money they didn't have, they had thousands upon thousands of researchers all over the world sending in their suggestions for solutions to their molecular problems, and they only had to pay for the ones they used. Now, that is SMART!

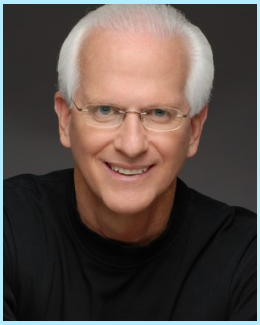
Do you see SMART opportunities in these statistics?

- About 66% of employees would take a lower paying job for more work flexibility.
- About 62% of employees believe they could fulfill their duties remotely.
- About 60% of employees believe they don't need to be in the office to be productive and efficient.

Could you lower overhead and expenses by having some people operate from home? Some managers will immediately say, "That won't work; you won't have control of your employees. They won't get things done." If that is your argument, my statement to you is this: you have hired the wrong people.

JetBlue has hundreds of reservation agents operating from their own homes. Their home -based agents save, on average, up to $4,000 on their commuting expenses, not counting the savings of lunch, daycare and wardrobe. JetBlue found they had a 25% increase in productivity once employees were allowed to work from home; they figured out a different, more productive, less expensive, more profitable … *SMARTER* way to operate.

To survive in this competitive marketplace, you must change, adapt, modify, challenge, innovate, transform, revise and improve, but what's paramount to your success is to be working SMART!



Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys *and* 52 Essential Habits For Success, *he's shared the podium with esteemed figures from across the US, including former President George H.W. Bush, former Secretary of State Colin Powell, Tony Robbins, Tom Peters and Stephen Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.*

These 6 Hobbies Will Make You Smarter

Play An Instrument – Learning to play an instrument – or playing an instrument you're already familiar with – keeps the brain sharp. It's an "active" hobby that creates new neural pathways in the brain, which is linked to good brain health, including improved memory and problem-solving.

Read Constantly – Reading helps reduce stress while boosting cognitive abilities, like interpreting data and emotions. Interestingly, it doesn't matter what you read as long as you read often.

Exercise Daily – Exercise promotes the release of brain-derived neurotrophic factor (BDNF) within the body, a protein that promotes healthy brain activity, including better mental acuity.

Learn A New Language – Like playing an instrument, learning a new language creates new neural pathways. Research shows that people who learn a second language

are better at solving puzzles and problems.

Play "Brain Games" – Activities such as sudoku, puzzles, board games and problem-solving video games can be beneficial to the brain. These activities increase brain neuroplasticity, which improves cognitive ability and reduces anxiety.

Meditate – It's also important to quiet the brain. Meditation improves focus and can improve your mood significantly, which can boost confidence. *Business Insider, Dec. 17, 2019*

Beware At The Gas Station…

If you use a credit card at the gas pump, you increase your risk of having your credit card information stolen. At the end of 2019, Visa warned a number of its customers that hackers are actively stealing credit card information by hacking into gas stations' point of sales networks. These networks, it turns out, are not as secure as they should be.

Hackers also use phishing scams. All the gas station employee has to do is click a malicious link and hackers can install software that steals credit card information from the station and sends it back to the hacker.

What can you do to protect yourself? Make sure your credit cards are up to date with the latest chip technology. Never use your card's magnetic strip, if possible. If you're still using your magstripe, ask your issuer for an updated card or find a new credit card provider. Cash is also a great option. *Inc., Dec. 16, 2019*

4 Ways To Improve Business In 2020

Automation – Boost efficiency with automation tools. Think accounting and financial management tools like FreshBooks and QuickBooks or project management tools like Trello. You can also use e-mail marketing apps like Mailchimp.

Accessibility – Make it easier than ever for customers to book your services. Online-scheduling software streamlines the process, allowing customers to schedule times that work for them and you. You can have customers book times on your website or Facebook page.

Employee Engagement – Delegate more, encourage more communication through apps like Slack and celebrate more achievements.

Customer Service – Chatbots and other types of similar customer service-based artificial intelligence are bigger than ever. Use them on your website or direct customers to Facebook Messenger. HubSpot's Chatbot Builder is a good tool to try when getting started. *Small Business Trends, Dec. 1, 2019*