5 Cybersecurity Threats

Your Business Can't Afford to Ignore

WSI

Let me ask you a question: do you think about your cybersecurity on a day-to-day basis?

If not, you're making a big mistake!

I'm a retired FBI Special Agent, and I've spent my entire career trying to thwart cybercriminals. For 12 years, I managed the FBI's Memphis Division Computer Intrusion/Counterintelligence Squad in Nashville. These days, I travel to events and conferences to share my knowledge and experience in hopes of preventing people and organizations from becoming cybercrime victims.

The message you are about to read in the pages that follow is extremely important. The issue of cybercrime is getting worse, not better. And contrary to mainstream belief, everybody – yes, even you and your business – is a potential cybercrime target.

With a little care, attention and a few no-cost preventative measures, you can go a long way to keeping your digital information safe.

5 Cybersecurity Threats Your Business Can't Afford to Ignore is the perfect resource for individuals and businesses looking to secure their sensitive information. I give it my full approval, and I highly recommend you read it and put WSI's suggestions into action.

GOOD LUCK AND STAY SAFE!

SCOTT AUGENBAUM
– RETIRED FBI SPECIAL AGENT AND CYBERSECURITY EXPERT

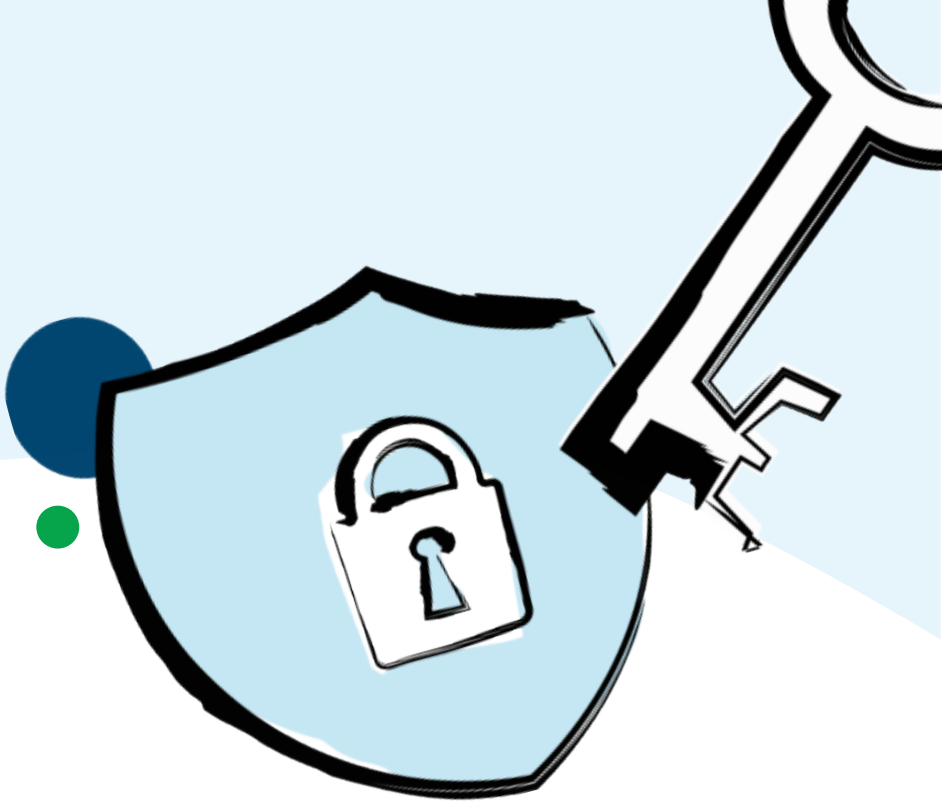


TABLE OF CONTENTS

Introduction 4

Everyone Is A Potential Cybercrime Victim (Yes, You Too) 5

Cybersecurity Self-Check: How Secure Are Your Accounts? 7

Once The Bad Guys Get Your Stuff, There's No Getting It Back 9

Failing to Use Two-Factor Authentication Can Put You At Risk 10

Cyber Criminals Prey on Weak Passwords 12

Cybersecurity Do's and Don'ts 14

Letting Your Guard Down on Social Media 15

Please Don´t Ignore Your Cybersecurity 16

Basic Cybersecurity To-Do Checklist 17

About WSI 18

Scott Augenbaum recently told a room full of marketers his job as an FBI Special Agent used to be easy to explain: he caught bad guys and put them behind bars.

20 years later, and things aren't so easy to explain. There are still bad guys out there roaming the streets, but in today's increasingly digital world, we're all targets of a new kind of theft: cybercrime.

Like most people, you probably don't give much thought to your cybersecurity (kudos to you if you do, you're ahead of the game). And as we've seen in the news far too often over the last couple years, many businesses aren't thinking about cybercrime either.

Our goal is simple: we want to teach marketers and businesses how not to be a victim of cybercrime. You've got cybersecurity content in your hands – or more likely, on your screen – so that's a great start!

Now we're going to dive right into the 5 cybersecurity threats businesses (and individuals) can't afford to ignore.

"Cybersecurity costs will reach 1 trillion dollars in five years - and it still won't be nearly enough to stop the bad guys!"

SCOTT AUGENBAUM

1 EVERYONE IS A POTENTIAL CYBERCRIME VICTIM (YES, YOU TOO)

One of the biggest reasons cybercrime is so prevalent is nobody thinks it can happen to them. Often, the low level of concern for cybersecurity stems from some common misconceptions about cybercrime.

Here are a few thoughts about cybersecurity that are unfortunately echoed by many eventual cybercrime victims:

"It will never happen to me, I have nothing of value."

Whether it's individuals or businesses, the most frequent response we get when we ask about cybersecurity is, *"Why would cybercriminals target us? We have nothing anybody would want!"*

Yet small businesses, non-profit organizations and healthcare companies are commonly targeted by cybercriminals. Many small companies have an unfortunate lack of concern for cybersecurity, or they believe they have nothing of value and therefore can't possibly be a target.

The truth is every individual and business has sensitive information they need to keep safeguarded.

"We have security measures in place, we're safe."

Think about your business and what confidential information you have access to. How do you keep it safe? You may have a firewall, an intrusion detection system, and other security measures in place that make you feel safe. But every business and individual uses common technologies that exist outside of basic protection.

Our personal and corporate email accounts can be used against us. Social media profiles are popular targets for cybercriminals because they can be used to infiltrate our network of family and friends. Even worse, cybercriminals can use a compromised account to infect a business's customers with malware. If that happens, you can kiss those clients goodbye!

What about the cloud-based applications most modern businesses use, like CRM systems and payroll applications? These databases contain mountains of sensitive information about a business's operations, clients and employees. The pieces of information stored in these systems also need to be properly protected, otherwise, they could become vulnerable.

"We have much bigger competitors. They'll get targeted, not us."

Additionally, companies with much larger competitors often believe they are shielded from cybercrime, because why would anybody target the smaller organization? This ill-fated thought process goes something like this, *"We're much smaller than those guys, we only have 5 million pieces of information – our larger competitor has 20 million. They will be the target, not us."*

Let's get these misconceptions out of the way right now. Whether you're an individual with five pieces of information or a global corporation with 50 million, you're a potential cybercrime victim. We all are, and it's only once we acknowledge and understand how serious cybersecurity is that we can begin to properly protect our data and information.

Cybersecurity Self-Check: How Secure Are Your Accounts?

This is a simple test. Answer each question below, and give yourself the corresponding number of points. At the end, tally up the points to find out how secure you are:

---

1. **How worried are you about your cybersecurity?**
   a) What's cybersecurity? *(1 pt)*
   b) Not worried at all *(2 pts)*
   c) A little worried *(3 pts)*
   d) Pretty concerned *(4 pts)*
   e) Worried and I need to be prepared *(5 pts)*

2. **On how many of your accounts do you use two-factor authentication?**
   a) What's two-factor authentication? *(1 pt)*
   b) I don't know, maybe one? *(2 pts)*
   c) One or two *(3 pts)*
   d) Three or four *(4 pts)*
   e) All of my mission critical accounts *(5 pts)*

3. **How many of your accounts have the same password?**
   a) All of them *(1 pt)*
   b) No idea *(2 pts)*
   c) A few *(3 pts)*
   d) One or two *(4 pts)*
   e) None of them *(5 pts)*

4. **Prior to doing this test, when was the last time you thought about your cybersecurity?**
   a) What's cybersecurity? *(1 pt)*
   b) Never *(2 pts)*
   c) Years ago *(3 pts)*
   d) Last month *(4 pts)*
   e) Yesterday *(5 pts)*

5. **If a cybercriminal stole your stuff, how likely do you think you are to get it back?**
   a) What's cybersecurity? *(1 pt)*
   b) Definitely getting it back *(2 pts)*
   c) Pretty likely *(3 pts)*
   d) Unlikely *(4 pts)*
   e) I'm never getting it back *(5 pts)*

6. **How would you rate the strength of this password:** *Iforgot123?*
   a) Very strong *(1 pt)*
   b) Strong *(2 pts)*
   c) Does the job *(3 pts)*
   d) Weak *(4 pts)*
   e) Very weak *(5 pts)*

Results Table:

30 Points

Wow, are you sure you aren't Scott Augenbaum?! Good stuff! Although it's unlikely your stuff is at risk, make sure you remain vigilant!

23-29 Points

You are a cybersecurity pro! There's a tiny bit of room for improvement, but you're far from an easy target. Keep up the good work!

16-22 Points

You show a healthy concern for your cybersecurity, but there's work to be done. I wouldn't be comfortable, if I were you.

9-15 Points

We're worried about you – you are a potential cybercrime victim. You're aware of cybercrime, but your level of concern is way too nonchalant.

8 Points or less

Your cybersecurity is as low as it gets, and you're at high risk of becoming a cybercrime victim.

We highly suggest you follow our *Cybersecurity Do's and Don'ts (page 14)* and implement the items on our *Basic Cybersecurity To-Do Checklist (page 17)*.

2 ONCE THE BAD GUYS GET YOUR STUFF, THERE'S NO GETTING IT BACK

Here we go, from a couple common misconceptions to a really unfortunate one. The first thing Agent Augenbaum usually talks about when he addresses rooms full of people is the fact that cybercrime victims never get their stuff back.

"Look, I work for the FBI. It's my job to stop and catch the bad guys. But here's the hard truth about cybercrime: once the bad guys get your stuff, and you call the FBI, or the police, we can't get it back for you. As soon as your information is stolen, it's gone."

– SCOTT AUGENBAUM

The harsh reality of cybercrime is that it isn't like getting your bike, your car, or even some items from your house stolen. There's nothing and nobody to track, and there's no insurance policy to cover your losses.

This is the reason businesses need to be proactive, not reactive, about cybercrime. The only reaction to having your identity stolen, or having the identities of your clients stolen from your possession, is to weep for your immediate future because you're in for a very long, frustrating and uncomfortable road to recovery.

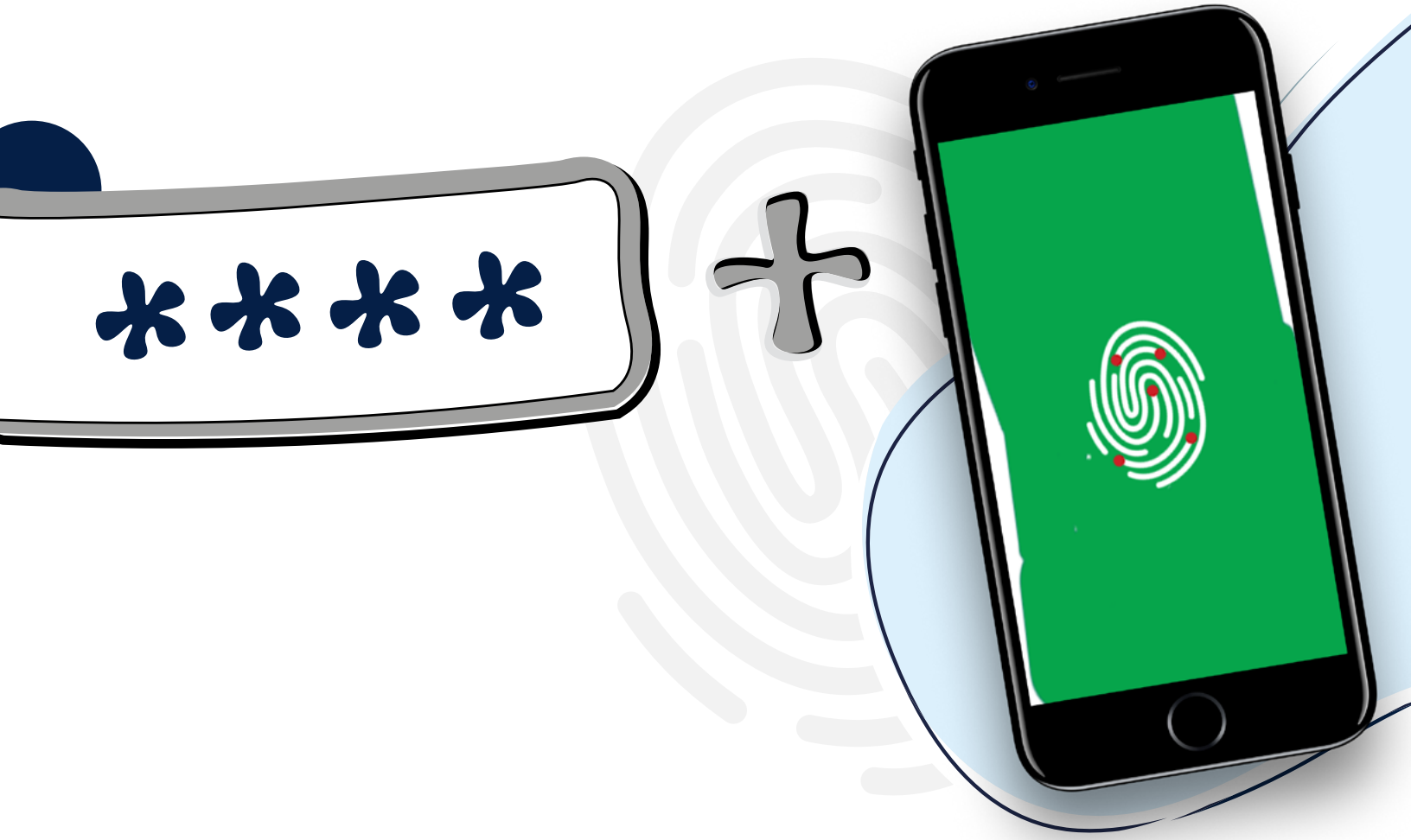
Businesses absolutely have an obligation to protect the online accounts, data and personal information of their clients. The CIA triad – confidentiality, integrity, and availability – is part of doing business, both now and into the future. A cybersecurity breach is not a mistake or an oversight, it's a failure that could have been avoided.

Organizations that don't take cybersecurity seriously will not only lose their stuff forever – they'll lose their business, too.

3 FAILING TO USE TWO-FACTOR AUTHENTICATION CAN PUT YOU AT RISK

So what is two-factor authentication technology?

Two-factor authentication is a method or technology that confirms a user's identity by any combination of two different factors: something they know (usually a password), and something they have (a text message sent to their phone) or something they are (voice or fingerprint).



For example, PayPal, the popular online payment system, requires two-factor authentication for all accounts. To access a PayPal account, you'll need your account password, and then you'll either get a code sent to your device via text or be required to answer two more security questions. Simple, but effective.

The next question, then, is why isn't everybody and every business using two-factor authentication? There are two main reasons, but neither of them is a good enough excuse not to use two-factor authentication.

The first is that it requires some minor effort to set up and use. But the effort is more than worth the payoff. Enter your phone number, scan your fingerprint and set those security questions, because each of them could be the one and only thing standing in the way of having your identity stolen.

On the business front, it's a given that organizations should require their employees to go the extra mile when setting up accounts. An issue that businesses sometimes have is finding applications that use two-factor authentication, or more commonly, struggling with the change from an outdated software to something newer, with better security.

It's understandable. Changing hundreds or thousands of users over from one application to another isn't easy. But again, it's worth the trouble, and it really isn't a choice. When it comes to cloud-based platforms and applications, businesses have to insist on working with companies and partners who use two-factor authentication.

The ***Two Factor Auth*** website is a great resource that provides an in-depth rundown of almost any digital software, application or account that a business or individual would want. Whether you're cross-checking that your applications use two-factor authentication or looking for a new one to replace something outdated, the Two Factor Auth site is invaluable. Check it out, and use it to audit your cybersecurity from top to bottom.

Did You Know? 85% of all data breaches could be prevented using two-factor authentication!

4 CYBER CRIMINALS PREY ON WEAK PASSWORDS

All it takes is one password, especially if you're like 70% of people who use the same password for multiple accounts. One password and the bad guys have all your stuff.

For businesses, it's as nonchalant as an employee creating one lazy password for a cloud-based account they don't think matters. One account becomes two, and before you know it, *"Password123"* is the business's default password for multiple cloud accounts. One spray attack later, and all the data is in the hands of, you guessed it, the bad guys.

A spray attack is relatively simple in theory, but it's deadly for anybody using weak passwords, or the same password for multiple accounts. In a spray attack, attackers try common passwords, like *"Password123"* or *"Iforgot!"* one by one, across thousands of cloud-based accounts they've identified as targets. The key to a spray attack is trying the same password on all the target accounts before cycling in a new password, so as to avoid getting locked out for too many failed attempts.

If this sounds frighteningly organized, that's because it is. But in the end, no matter how good the cybercriminals are, businesses and individuals can thwart cyberattacks using only two-factor authentication and strong passwords.

There are a few easy rules to follow:

- **Have separate passwords for mission-critical accounts like:**
  - Bank accounts
  - Email accounts
  - Cloud accounts
  - Client data
  - HR systems
  - Payroll
- **Don't use weak passwords for anything**
- **Come up with a password creation system and use it OR**
- **Find a password management tool with two-factor authentication**

For the password creation system, Scott Augenbaum recommends the following criteria:

- **12 characters in length**
- **Both uppercase and lowercase letters**
- **Special character and a number**
- **Personal passphrases**

For example's sake, here's how to create a password using this system.

Start off by picking a special character and a number, like #9. Now flip the character and the number – 9# – and these two sets will bookend your password, so it will look like this: #9_____9#.

Next, think of an eight-word passphrase that has personal meaning. For example, "Toronto Maple Leafs will win the Stanley Cup." Now take the first letter of each word in the passphrase, keeping the case the same: TMLwwtSC.

Put everything together and we have our strong, uncrackable password:

#9TMLwwtSC9#

While this might seem difficult at first, it actually gets easier the more you do it. And one thing is for sure: the bad guys want easy targets, so if this is how you're protecting your accounts, they'll want nothing to do with you.

Cybersecurity Do's and Don'ts

Do's

- Use service providers that offer two-factor authentication.
- Use our password creation system to generate mission-critical passwords.
- Use different passwords for mission-critical accounts.
- Use different passwords for as many of your accounts as possible.
- Think before you click, no matter what you're doing online.
- Protect yourself on social media.

Don'ts

- Never believe that it can't happen to you – it can and it will.
- Don't assume the FBI, or anybody else, can get your stuff back.
- Never use a service provider unless they offer two-factor authentication.
- Don't use the same password for mission-critical accounts.
- Don't get complacent about your cybersecurity.
- Don't let your guard down on social media.

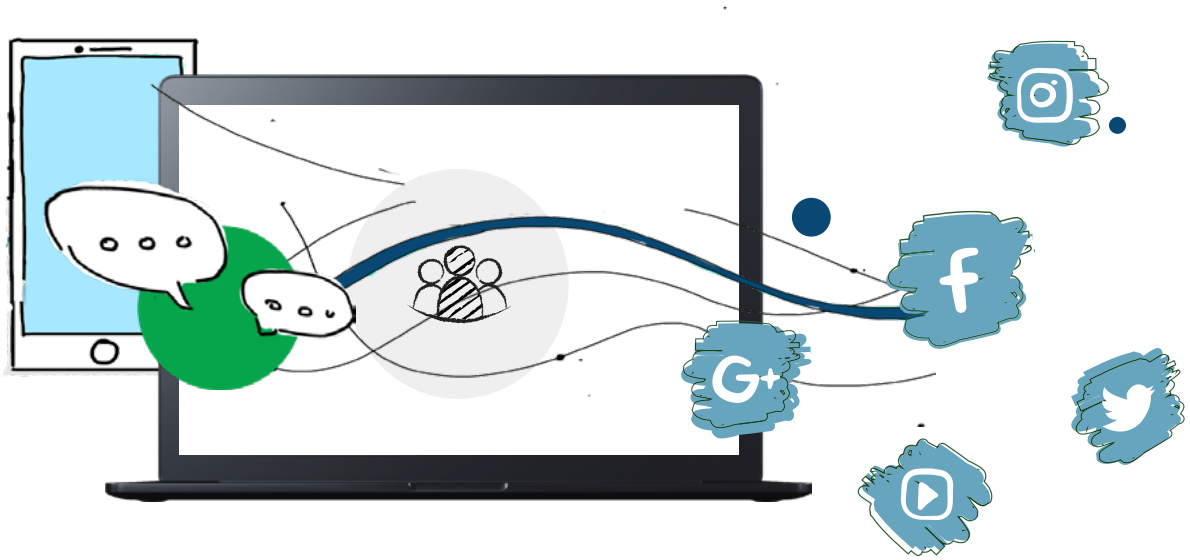
5 LETTING YOUR GUARD DOWN ON SOCIAL MEDIA

For most of us, social media is part of our everyday lives. Even in the business world, social media has become an integral component of digital marketing strategies.

Despite social media's prevalence in our society, there is still an alarming lack of concern for safety and security on social media. Many of us don't care about our privacy on social media; how many of your accounts are private, for example? We also don't think twice about security, often using our social information to log in to third party accounts and applications, without a second thought about what information and access we're giving to these third parties.

Being lazy or nonchalant with your social media is a huge mistake. Cybercriminals think of social media platforms as a gateway to your more valuable personal information. Whether it's taking advantage of the fact that some people use the same password for Facebook as they do for their bank account, or simply gleaning valuable personal details such as a job or an address, social media profiles are a treasure trove of information for cybercriminals.

Do not let your guard down on social media because it could be the area where you're most vulnerable.



Please Don't Ignore Your Cybersecurity!

The consequences of not giving cybersecurity enough time and attention are extremely costly, for both businesses and individuals. But, if you're willing to put in the effort and take action on our suggestions, you can secure your digital data for both yourself and your company.

Here are three main takeaways we'd like you to remember. They are non-technical, and they don't require you to buy anything, so there are no excuses.

1. **Think before you act. Think before you click. You are your own firewall, so question everything, and if you aren't sure, don't click.**

2. **Don't do business with people or companies that don't use two-factor authentication. Period. No exceptions.**

3. **Use strong passwords, and don't use the same password for two different mission-critical accounts.**

We can't make a guarantee about things beyond our control, but we can say this: if you're conscious of these three things, you're well on the way to securing your information, and should remain safe from hackers and cybercriminals.

To end things off, we'd like to offer our this checklist of things you can do, right now, to start immediately improving your cybersecurity. This is not a complete, exhaustive list, but if you start checking these things off you'll be more secure than you were yesterday!

Basic Cybersecurity To-Do Checklist:

- [ ] Make a list of at least five of your "mission-critical" accounts.
- [ ] Ensure the service providers for these "mission-critical" accounts offer two-factor authentication.
- [ ] If two-factor authentication is not offered, either find a new provider, or ask the current provider to implement two-factor authentication.
- [ ] Use our password creation system to generate a different password for each "mission-critical" account.
- [ ] Think before you click or act.
- [ ] If you're a business owner, inquire with your IT team on the level of security of your data management systems.
- [ ] Review the privacy settings for your social media accounts.
- [ ] Keep your cybersecurity top of mind and don't get lazy – this is what cybercriminals depend on.
- [ ] Encourage your family and closest friends to use this checklist – send it to them if you have to!

We're a powerful network of marketers who strive to discover, analyze, build and implement digital solutions that win digital marketing awards and help businesses succeed online.

Headquartered in Toronto, Canada, WSI is a digital marketing company with a strong international presence. Our Digital Marketing Consultants use their knowledge and expertise to connect their clients with their customers online.

We're a powerful network of marketers who strive to discover, analyze, build and implement digital solutions that make a difference for businesses all around the world.

Over the last 20 years, WSI has won multiple digital marketing awards for our solutions by adapting to the constantly shifting landscape of the Internet. We take pride in helping businesses make the most of the dollars they spend on digital marketing.

Ready to move ahead and discuss a project with a local Digital Marketing Consultant?

Get in touch with one of our experts now by visiting ***www.wsiworld.com***