Protecting Your Digital Life: How to Stay Safe in a Connected World

Thank you for attending the webinar, "Protecting Your Digital Life." You made the right decision to educate yourself on common cyber threats and ways that you can be safer online.

Use this webinar transcript as reference to help you TAKE ACTION. ☺

1. TITLE: Protecting Your Digital Life

Hi Everyone. My name is Jane Scandurra and I want to thank you for joining this webinar today about an important topic we should all be very focused on – and that is, protecting our connected, digital lives.

We all spend a lot of time connected to the internet in one way or another. We have become increasingly dependent on – and for some, even addicted to -- our various devices – whether it be laptops, smartphones, televisions or popular personal assistants like Amazon's Alexa or Google Home.

I'm just like everyone else in that regard. But I've also become super diligent about security and privacy. And that's why I'm here today to help you become that way too.

Everyone knows the risks. It's in the news a lot lately. But I've found that regardless of that, too many people don't have a sense of urgency when it comes to making the time to put safeguards in place – until after they experience a privacy breach or full out attack on their digital life – which, of course, is too late!

If this sounds like you, you made the right decision to be on this webinar today.

A little bit about me and why ***I*** am here today….

2. Digital is in my DNA

That's me sitting at the typewriter. I'm in my father's office in Queens, NY, many moons ago. It looks like I'm about 8 or 9 years old. Little did I know back then that I'd spend so much time in front of a keyboard for decades to come. But boy is that a reality.

I know what the world was like before the digital age. I may not have been born during the digital age, but most of my adult life has been spent working in the online industry. Living digital is in my DNA. And having the context and perspective of both the before and after worlds gives

me a unique perspective of navigating through it. I've achieved great benefits as a result…and I've witnessed a lot of the risks, weaknesses and what can go wrong.

3. Digital is in my DNA #2

I started working in the online industry over 30 years ago, at a company called Prodigy, which was a joint partnership of IBM and Sears. I'd like to say I started working there right after this photo of me at the typewriter was taken, so you don't think I'm that old, but sadly, that's not the case.

At the height of its success, Prodigy was the largest online service in the US, prior to the commercialization of the Internet. My colleagues and I were true online pioneers. At the time, it was actually quite funny trying to convince people that yes, they could shop on a computer – and yes, soon everyone would own a computer in their homes. That's how far back it was.

After Prodigy, I worked for IBM. Because of my unique experience in the online industry, I was hired into their newly formed Internet division and went on to hold various global marketing management roles over 11 years.

Now I run my own consulting and training business. Just for fun, I also co-produced a feature documentary film about 10 years ago. My experience in online networking and social media marketing helped the film get featured in various national media over the years – print, radio, and tv. That's me in the red dress being interviewed by Kathie Lee and Hoda on The Today Show with the Publisher of More Magazine. Fun stuff.

Point here is, I have experienced quite a lot in the digital, connected world – both the massive benefits it offers and I've seen a lot that has gone very wrong – particularly regarding privacy and security – and the concerns have only become magnified over the years.

My company, Scandurra Group, is also proud to be an official partner of Stop.Think.Connect. the global online safety and awareness campaign from the National Cyber Security Alliance.

So, I'm passionate about helping others become more aware of the ways that they can safely enjoy their connected time.

4. Objective: Awareness & Action

My consulting business focuses on helping organizations around the world thrive in the current attention starved economy with digital marketing and social selling strategies.

Helping people pay attention to cyber safety fits right in with that, so I am delivering this webinar as a public service – for the greater good of all, because protecting our digital lives is a shared responsibility.

Something that you do – or don't do – online can very well impact not just yourself, but also the safety of friends and family that you are connected to.

So, if you get value from this webinar, I hope you'll share the registration link with others so they can benefit as well.

Let me be clear: This webinar is not a sales pitch. No cyber security software, no silver bullet gimmick, promising guaranteed protection from the bad guys – because that doesn't exist.

But if you'd like to follow me or contact me to help keep you motivated on cyber safety practices, I welcome that.

I'll give you different ways to do that later in the webinar. I'll also give you an opportunity to get a full transcript of this webinar for reference – but you'll have to stick around to get it!

The content I'm about to share might scare you a little, especially when you learn about current threats out there that you might not be aware of – and the many safety practices you're not doing – or putting off for another day.

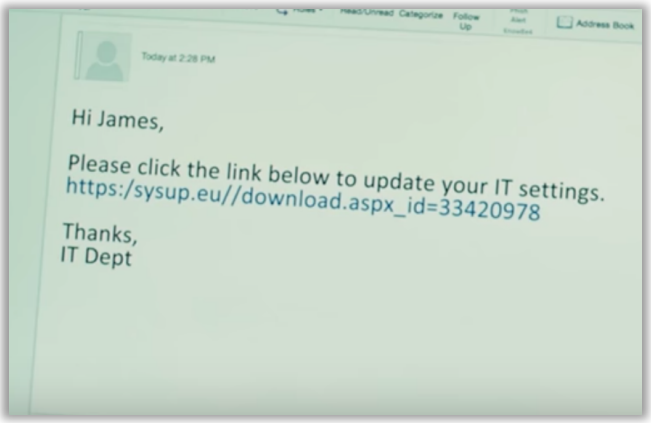
That's not the objective – although it might be necessary – because my ultimate objective is not just to make you more aware, but for you to take ACTION so that you can be safer online. That will give you more peace of mind that you are doing your best to keep the bad guys from scamming you.

So, to start, let me set the stage with a very real scenario that could happen to any one – but it's more likely to happen to someone who is not actively following the cyber safety tips that I'll be sharing with you today…

5. Imagine this scenario

Imagine that you're going about your regular life with your daily routines. One of those daily routines is checking your email in the morning when you get into the office.

One morning, within the sea of new mail in your inbox, you get an email from your company's IT department– like the one you see here - asking you to update your settings.



Just as you open this email, a colleague comes by your desk and asks if you want to grab a quick coffee and catch up on a project you're working on together.

You'd love another coffee and you think – perfect timing, you can have the system update your settings while you're gone so, without much further thought, you click on the link in the email and head out for coffee.

When you return, this is the screen that appears on your computer. The email you received, LOOKED like it was from your IT department, but it was NOT from your IT department. It was a phishing scam and you just become a victim of a ransomware attack.

Phishing, spelled with a ph, not an f, is a type of online scam where criminals send an email that appears to be from a legitimate company and asks you to provide sensitive information.

Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge – like in the scenario I just described.

The concept behind ransomware is simple: Lock and encrypt a victim's computer data, then demand a ransom to restore access. In many cases, the victim must pay the cybercriminal within a set amount of time or risk losing access forever.

And since we're dealing with criminals here, paying the ransom doesn't even guarantee access will be restored. Plus, the payment is usually demanded in Bitcoin. I don't know about you, but I wouldn't even know how to get bitcoin to pay the ransom, if I truly had to.

9 out of 10 phishing emails in 2016 contained a ransomware payload. And not long ago, a global cyberattack spread ransomware to computers over 150 countries. This is serious stuff. It can happen on your personal devices at home or on company owned assets at work. Cyber attackers play no favorites.

If backup copies of your files don't exist, then you have a difficult decision to make: Can you afford to move on without access to your files, or do you have to consider paying the ransom?

While the general advice is not to pay, there have been cases where disruption caused by ransomware have been severe enough to effectively bring an organization grinding to a halt.

Because ransomware infections have such an immediate and damaging consequence, that puts the emphasis on preventing attacks from happening.

One good way to prevent is to stop and THINK – and investigate -- before you click on ANYthing that looks even remotely suspect.

This is just one scenario of a potential cyber attack on your digital life.

6. Realities of a connected world: greater opportunities, greater threats

That was a scary scenario, I know, but it's reality. Technology is driving more change in the world than ever before, and with that change comes more opportunities for growth,

convenience, entertainment. But on the flip side, as we continue to adopt new devices and technology, we're opening ourselves up to more opportunities for cyber attacks.

The real challenge, though, may be that avoiding technology just isn't an option in this day and age. We all want to interact through digital channels; every single company in every single industry is in some state of digital transformation – or should be if they want to remain competitive in the 21st century.

Technology is a double-edged sword – rich in possibility but also leaving users prone to attack. So, what can you do to maximize the former and minimize the latter?

Education is big part of the solution. Educate yourself. Educate your colleagues and employees. Educate your friends and family. That's the purpose of this webinar.

Information is the currency of the 21st century which the bad guys are after. But with more and more devices becoming internet enabled, criminals are set on conquering a whole new internet-connected frontier.

7. Cyber attackers rely on human error

We now live in an attention starved world. And when you're not present….when you don't pay attention, when you're moving too fast, you're apt to make mistakes…or frankly, do something stupid.

And not surprisingly, cyber attackers live for that. When we're complacent or we're not paying attention or we do stupid things, we're more vulnerable.

Frequently, cybersecurity breaches stem from human error. Other attacks happen because you may not know about helpful cyber safety practices.

It happens every day—people open emails from unknown senders, click on mysterious links out of curiosity, and even print out sensitive information at work and leave it sitting on the printer.

These actions are not uncommon. But they **are** PREVENTABLE actions. Studies have shown that human error or behavior is the cause of 90% of business cyber attacks.

Most people actually claim to be aware of the risks. But just because they're aware of the risks, doesn't mean that they always follow best practices.

But that's all going to change for you today after this webinar, right?

Because when one of us is careless online, ALL of us can become vulnerable by their actions. Like it or not, we are all connected in one way or another.

We all need to help each other be more diligent in acting more responsibly online.

8. Your best defense is common sense

Cybercriminals use a wide variety of scam tactics in order to gain access to a device or network, extort money, or steal valuable information.

Here's the good news: attention and COMMON SENSE is actually your best defense. That goes for navigating online as well as navigating traffic on busy streets.

It's hard to imagine day-to-day life without the option of doing so many things online. But every online portal opens the door to potential danger from cybercriminals that want to steal your money or your identity.

Prevention starts when you feel that something isn't right. Follow your intuition.

For emails, the giveaway may be an email address that doesn't match a company name, a request to "confirm" or "update" information that a company should already have or a notification that a financial account was "suspended" without warning. The email may also have misspellings or grammatical errors.

When hackers create a fake deadline within the email or use wording that creates a sense of panic, such as "your account has been suspended, their purpose is to get you to act before you discover the fraud.

If you have even a single doubt that an email, a text, a phone call hasn't come from a legitimate person, it's worth investigating further. A little extra time spent checking can save a lot of heartache – and potentially money – later on.

So, let's talk about what you can do. Again, let me say that none of us will ever be 100% safe from threats, but there are many simple, common sense practices that can make you a lot safer than you may have been before attending this webinar today.

9. Create strong passwords

Did you know that Kanye West's iPhone password is six zeros? We all do, since TV cameras caught him unlocking his phone during a meeting in the Oval office with the President. Six zero's is NOT a secure password. Neither is 123456 – although it's probably just as common.

Sure, it's much easier to remember and to enter quickly when you're busy, but one of the most common ways that hackers break into computers is by guessing passwords. Simple and commonly used passwords enable them to easily gain access and control of a computing device. You may as well just hand over your digital life to criminals if you do this.

On the flip side, a password that is difficult to GUESS makes it very difficult for common hackers to break into a machine and will force them to look for another target. The more complex the password, the lower the likelihood that your computer or device will fall victim to an unwanted intrusion.

For starters, DON'T use standard number substitutions like the one you see here in yellow type. Think that version of "P455w0rd" is a good password? N0p3! Password cracking tools now have those built in.

Don't use a SHORT password—no matter how weird it is. Today's processing speeds mean that even the most obscure, 6 character passwords are quickly crackable with a software programs hackers use. Your best defense is the longest possible password.

This is very important.

Passwords that are long and complex require more effort and time for a hacker to guess.

Passwords should contain at LEAST ten characters and have a COMBINATION of characters such as commas, percent signs, and parentheses, as well as upper-case and lower-case letters.

Also, don't reuse passwords. If you do, and a hacker gets access to just one of your accounts or one of your devices, they will try to use the same password to take control of others – and eventually own them all.

One of the concerns that people often have when it comes to creating complex passwords is a fear of forgetting them, particularly when there are several to remember. Naturally, a person should try to think of something that will be easy for them to memorize.

One way to do that is to turn a sentence or phrase into something that is not easily recognized by others. Something really unusual, but memorable –

LIKE… I eat lasagna with pickles. Of course, I don't – and wouldn't dream of doing it – that combination would taste horrible. But that combination is weird enough not to be guessed by a hacker either.

Or take a long sentence and use, use the first letter of every word in the sentence, replacing certain words with numbers or symbols. And then add a prefix or suffix code for each account type to make each password truly unique. So, in theory, you will be using the same password, which makes it easier to remember, but you're modifying it to make it unique for different uses.

Never write down your passwords and leave them around the office - and for God's sake, don't put them on a post-it note and stick it to your laptop for anyone, including the office's night time cleaning crew, to see.

10. Hawaii Password

Remember when that false alert warning of an inbound missile was broadcast in Hawaii back in January 2018?

Shortly after that incredibly alarming event, people discovered that this photo that was taken in Hawaii's Emergency Management Agency for a news article in July 2017 includes a sticky note with a password.

Hawaii said the false alert was sent was because an employee pushed the wrong button not because of a hack, but the photo rightfully sparked criticism about the agency's level of security.

So, again. Use your common sense. Protect your passwords. They're the keys to most – if not all – of your digital life.

11. Sign up for multi factor authentication

The standard "username and password" approach to security is the practice we all depend on today, but it's still easy prey for cyber criminals. Many log-ins can be compromised in minutes, especially if you don't have long complex passwords.

I would suggest an extra layer of protection – on top of those strong passwords – that I KNOW you all will be implementing after this webinar.

Enable two authentication when it's offered, whether it be for accessing online banking, your Gmail account, your healthcare information or any other service you connect to, but particularly those that store sensitive data.

This adds that extra layer of security that helps to address the vulnerabilities of a standard password-only approach.

Two-factor authentication is a method of confirming a user's claimed identity by using a combination of *two* different factors:

1) something they know (like a code), 2) something they have (like a mobile phone), or 3) something they are (like a finger print or retina scan).

Using two of those three would be considered two factor authentication.

A good example of two factor authentication is when you withdraw money from an ATM; only the correct combination of a bank card (something you have, or physical possess) and a PIN code (something that you know) allows the transaction to be carried out.

Another example of two factor authentication is frequently used for many online services. Every fresh login would ask for the password & then a system generated one time four-digit code – which would be sent to the registered mobile number or email-id on the account. The extra code is something you KNOW, and it is sent to your device – which is something you HAVE.

This is good added protection. If a service offers it, use it. It may take you a few seconds longer to log into your account, but it's worth it.

12. Keep all software updated

It's happening again. That pesky pop-up message you see here is staring at you, telling you to update your software, begging you to make a choice: update or "remind me tomorrow."

What do you do? You choose the very tempting "remind me tomorrow", but we all know what that means.

I know, when I'm busy, I have been guilty of clicking that button a few times before finally stopping whatever I'd rather be doing to update my system. That's not a wise practice for me or for you.

That's why I'm here to tell you why keeping your software up-to-date is an important thing to do.

First and foremost, updates keep you safe from known security holes.

This is especially important when there is a new release available for software you use frequently, because most change logs and update notes reveal previously-known exploits that have already been patched.

Public knowledge of these exploits leaves your application easy prey for malicious users who are out to take advantage of these now known issues.

If you don't do the updates – or the longer you wait to do it -- it leaves your system open to compromise making your software vulnerable. Updating your software usually provides feature and speed enhancements as well.

Maintaining performance and security is crucial and it's as simple as pressing "update" next time that pop-up notification is blinking at you.

You might want to consider enabling settings to automatically install updates to ensure that you're fixing the identified weaknesses in the applications as soon as possible.

Although they're annoying when you're busy, there's a reason why updates are done, and they're usually to prevent malicious actions.

Try to make delaying updates a thing of the past.

13. Back up important Files

Remember that scenario I described just a few minutes ago with the ransomware attack?

What if that, God forbid, happened to you? What if your computer was seized and your files were no longer accessible or, even worse, destroyed forever?

There are other causes for data loss besides hacking -- machine breakdown, power outage, fire, flood and just plain human error.

It is very important to do regular backups to prevent the loss of data. Software can be reinstalled but your data could quite possibly be lost forever.

Aside from important documents, omg, think of all the digital photos you've taken of precious memories that could be gone forever.

We all know this. Do we all do back ups? Most likely, no.

Unfortunately, the regular process of backing up important files is too often put on the back burner just like updating software. Make that practice stop today.

There are a number of ways that you can back up your data.

You can back up your files to a cloud storage service like Dropbox or iCloud. Cloud Storage is a service where data is remotely maintained, managed, and backed up. The service allows you to store files online, so you can access them from any location via the Internet.

If you have a Mac, implement the TimeMachine feature. It's a built-in backup application used to keep an up-to-date copy of all of the files on your Mac.

Time Machine is unique among most backup applications in that it captures exactly what was on your Mac on any day in the past, making it easy to recover files, emails or media that may have been inadvertently deleted.

It might seem like Dropbox alone (or other online file syncing and sharing services, like Google Drive) are good enough for back up, but online options can fail too, or be hacked, as we know.

The cost of offline storage has plummeted over the years. In addition to using a cloud storage service like Dropbox, it might be prudent to also get an external hard drive to back up all your data – maybe even two drives – and keep them in different places.

If the house burns down, how will you get your memories or important documents back?

Just some things to consider – only you can decide how much of your data is that important to ensure there's back up access as well as some redundancy…. but the bottom line is that backing up your data is a good practice.

14. Manage your apps proactively

With all the advances in technology coming at is, it's fun to download new apps and try them out. I just started using a transcription app that can transcribe a webinar like this one into a fully annotated word document, in less than 5 minutes. Amazing.
Apps provide a lot of wonderful capabilities, but they are a common way that malicious actors disseminate malware or gather information about you.

Know that downloading ANYthing from the web comes with the inherent risk of infecting whatever it's downloaded to.

Always make sure you trust the app provider. Download the app from the Google Play Store, Apple's App Store, or other trusted sources, because they proactively remove known malicious apps to protect users.

All apps are not equal. Some have data collection as their primary reason for being —that's how they make their money. Some apps, on the other hand, collect almost no data at all. Some are free to use, some require you to pay to use them.

Something I always like to remind people, "when the service is free, you are not the customer, you are the product."

Before you install an app, you should do some evaluation and investigation. What information can it collect? What permissions does it ask for, and why? Which company or group is behind it, and can you trust it?

For the apps you decide are worth keeping, make sure you control their permissions.

Does that new calculator or flashlight app need access to your personal contacts to function? Hell no. On both iPhone and Android, you can control permissions either per app or by type of permission.

A few extra minutes of review can make a big difference in your safety.

Look at your smartphone right now. How many of those apps on your home screen are you actively using? I bet at least 20% of them are not being used.

I highly recommend reviewing your apps right after this webinar.

(no, not right now – I want your full attention here).

Disable or uninstall certain features or apps that you no longer use.

One last important thing about APPS….

We'll talk more about Wi-Fi in just a minute, but I suggest that you turn off Wi-Fi and Bluetooth when you're not using them.

Your phone uses Wi-Fi and Bluetooth to announce itself to networks and devices in its vicinity. They can also provide an easy way for a nearby, unauthorized user to gain access to your data.

Does your device automatically connect to public WiFi or other devices by default when you're on the go? It does if that's how you have it set up.

Do you want that? NO you don't. So fix it.

Make Wi-Fi and Bluetooth connections a proactive manual process.

There isn't any one thing you can do to make your smart phone more secure —rather, it's a lot of little steps and decisions.

Which I KNOW all of you are going to start doing as of today, right?

15. Use public WiFi wisely…or NOT AT ALL

Now more about public Wi-Fi. It's super convenient when you're on the go, right? Well, I don't ever use it and I would recommend that you don't either.

Despite numerous warnings, headlines, and efforts to educate, many people still don't understand why connecting to free WiFi is an incredibly dangerous situation regardless of what you're doing online.

And while you may think 'okay, I'm not checking my personal email or logging into my bank account, I'm just checking the news or sports scores,' remember anything you do on a public WiFi network is NOT secure. Any information you share or access on these networks is as good as gone.

If you absolutely must use a public WiFi network, avoid touching any personally identifiable information like banking information, social security numbers and home addresses at all costs.

Or, better yet, get a VPN -- or Virtual Private Network. A VPN is just what the name implies – a VIRTUAL PRIVATE NETWORK – where your online activity is private and secure.

A VPN allows you to create a secure connection to another network over the Internet. VPNs can be used to shield your browsing activity from prying eyes on public WiFi and more. They are an excellent alternative to public WiFi networks.

And while they do cost some money, the peace of mind and additional security is well worth it.

16. Guard against identity theft

Why would I have a photo of little girl on a slide about Identity theft?

Because identity theft isn't just an adult problem. Kids are victims, too.

In fact, more than 1 million children were victims of identity theft or fraud in 2017, according to a report from Javelin Strategy & Research.

And this added stat will shock you: Two-thirds of those victims were age 7 or younger.

So, if your toddler receives a jury-duty summons in the mail, or debt collectors start calling for your ten year old, don't be so quick to dismiss those interactions as a quirk of mistaken identity.

While adults make prime targets for their account balances, the "blank slate" a child provides can enable a criminal to do more damage by opening new lines of credit before someone catches on.

There's a lot of value in that there's no credit report tied to that Social Security number.

You might think that being 5 years old would be a pretty good "It wasn't me" defense against a fraudulent five-figure credit card bill. But experts say untangling identity theft and fraud committed against a minor is just as complicated as when the victim is an adult. You'll still have to go through the same steps with the bank or creditor to prove the fraud.

So, keep any sensitive personal and financial information out of sight. Because minors are much more likely than adults to become victims of FAMILIAR FRAUD – meaning the identity theft is someone they KNOW.

60% of child victims personally know the perpetrator, compared to 7 percent of adults. Family friends were the most common suspects, accounting for a third of cases. So just be aware.

Again…Be alert for unusual calls or mailings that would point to an adult problem, like a jury summons, collection calls or a rush of preapproved credit card offers.

You can protect yourself by taking these low-tech, common-sense precautions:

Store financial account statements, medical records, and tax filings and other sensitive information in a secure place at home, especially if you let workers or others inside, and shred those documents when you no longer need them.

Here’s another thing that I have personally found helpful and valuable in safeguarding my own identity.

If you’re not planning to buy a house, a car, or apply for a loan anytime in the near future, place a security freeze on your credit reports at the big three credit bureaus: Equifax, Experian, and TransUnion.

Doing this will prevent anyone from looking at your credit report except for the companies that already have a financial relationship with you, certain government agencies, and other exempt entities.

Once a hacker gets access to enough of your personal information to pose as you, they will likely try to attack your financial assets – by opening a credit card or applying for a mortgage or big loan – all of which requires a credit check – which will be denied if your credit access is frozen.

To sign up for a credit freeze, go to each bureau's home page and look for the security-freeze link. It's free.

You can easily un freeze them when you need to – like when you're buying a car or a new home, which require credit checks from reputable authorities.

17. Shop online with caution

More about identity protection….Shop online with caution. Before you enter your credit card information, check to make sure that the web site URL begins with HTTPS which indicates a secure, encrypted connection – NOT just HTTP.

Imagine that, just a quick, less than one second, glance can help keep you safe. You just have to remember to do it! Now you know.

Monitor accounts often. It's no longer enough to wait for your monthly credit-card or checking account statement to look for suspicious activity.

Hackers can now replicate active credit card numbers through random number generation software programs. They test them by buying something, usually in low dollar amount, so you won't notice and if they go through, they charge more and….lucky you, you get the bill. So keep your eye on your accounts.

18. Protect your social security number

Never give your Social Security number or other information to strangers who call, text, or send e-mail messages to you, even if they seem legitimate, as with phony "phishing" e-mail that looks like it comes from your bank.

If fact, don't give out your Social Security Number to ANYone unless it's your bank, doctor or other verified authority – and preferably only when YOU initiate the contact.

I'd love to get a bigger discount at my favorite clothing stores by signing up for their branded credit cards – but I'm not writing my social security number on a paper form and handing it over to a store clerk. Where are they putting it after I leave?

Again, use your common sense.

19. Create a separate "spam" email id

We all know how it goes….

You sign up to receive a free newsletter or to take advantage of a great offer, then before you know it your email inbox is getting stuffed chock full of spam, phishing emails and various other kinds of junk.

It happens to all of us.

The fact is, once you use your email address to sign up for almost anything, it ends up on every junk mail list known to mankind. The junk starts flowing in like water out of a fire hose, and you'll find that it soon becomes a chore just wading through your new emails every morning!

There is an easy way to avoid this scenario…Simply set up a "junk" email account with one of the free online email services, and use that email address to sign up for newsletters and special offers.

From that point forward, this new junk email account will be the unhappy recipient of all the spam, including potential malicious emails, that would have otherwise started landing in your primary email account.

Here's another good safety practice involving emails:

I would recommend using a unique, secure email address for password recoveries. It's inevitable, we all forget a password now and then and have to request to have it reset.

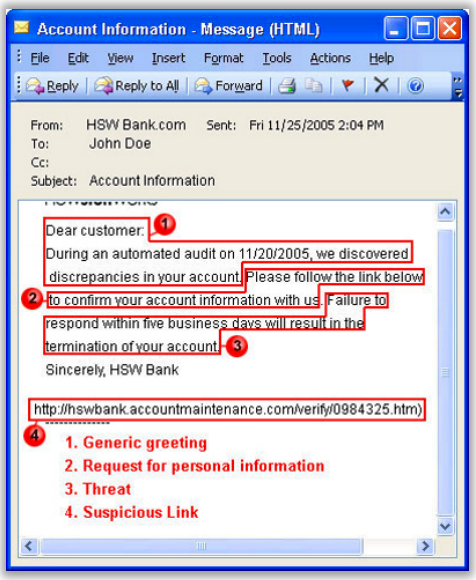
If a hacker knows where your password reset goes, that's a line of attack. So create a special account you never use for communications. And make sure to choose a username that isn't tied to your name, so it can't be easily guessed.

20. Don't fall for malicious emails…

We've said that human error is the most common reason for cyber breaches, so learn to spot the bad guys. And don't fall for their tactics which are getting more sophisticated and more authentic looking.

When in doubt, STOP and check it out.

Look at this example on the left.



It has a generic greeting. If you get an email from a company you have a relationship with, it's usually personalized with your name.

Request for personal information: Most, if not all, companies will never prompt you for your information via email or text. When someone does, this should be considered a red flag that they're not who they say they are. Check their email address or phone number and compare it with the person or organization they claim to be associated with for inconsistencies.

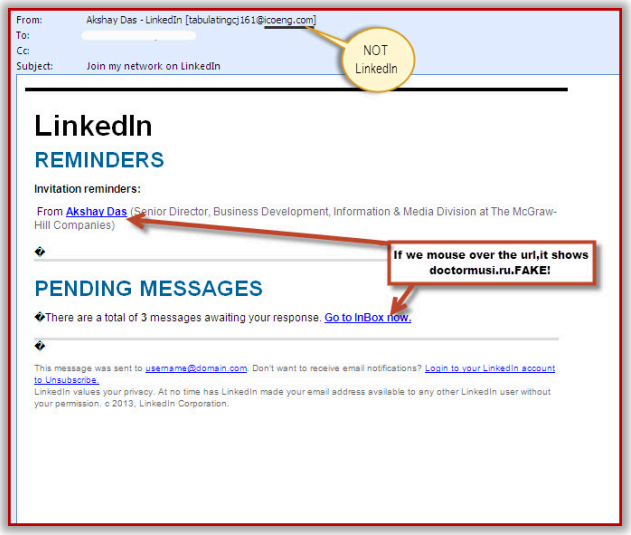
For example, if you get an email that looks like it came from HSW Bank, like this one here, physically GO to the company's web site and log in and see if there's a request for information there. Or call their customer service phone number on their web site – not any numbers listed in the email received.

Look for aggressive behavior: If the subject matter and language of a message is overly aggressive, it is likely a scam. Like this one saying that if you don't respond within 5 days, your account will be terminated.

The goal here is to make you uneasy, panic, and take the action the scammers want. Instead, check with the party they claim to represent before taking any immediate action.

Suspicious links -- if there are links, look for a reputable domain name as part of it. This one here on the left clearly screams scam.

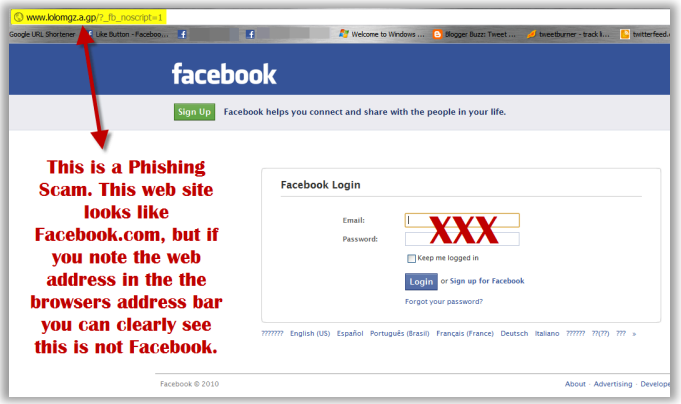
In the example on the right, if you hover over a hypertext link, you can see the web site destination of that link. Clearly, this example is showing a scam link as well.



Look for misspellings and poor grammar: Professional organizations take the time to read their communications over before sending. Oftentimes, phishing cybercriminals do not. If you receive a message from a supposedly trusted source that includes typos, poor grammar, or bad punctuation, chances are it's a scam.

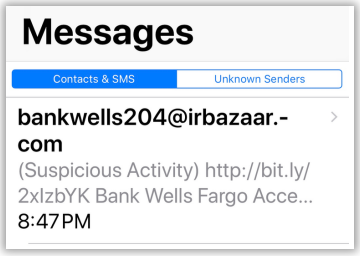
Just taking a few minutes on these sorts of things can make all the difference. Unfortunately, you may still get an obvious mass spam email from a self-proclaimed "Nigerian prince" from time to time, but the truth is many of today's phishing emails are surprisingly sophisticated.

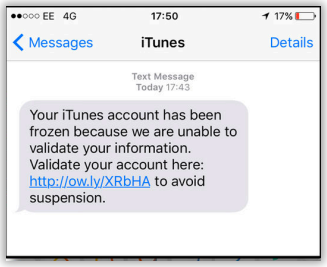
21. … Web sites, texts, phone calls



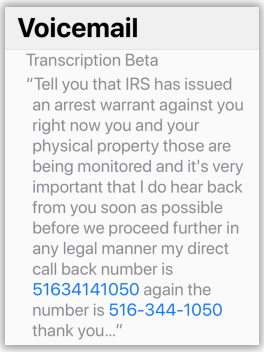
This web site on the left LOOKS like Facebook, right? But just a quick glance at the actual URL of the site shows that it is not. Don't be fooled. Look before you click.

On the right, are a few examples that I've personally received – ON MY CELL PHONE.





Yes, scammers have moved on from email being their communication vehicle of choice to text messages and even robo calls that leave threatening voice mails, like this one – that says the IRS is looking for me. I don't think so.



22. …messages telling you to copy and share with all your contacts

If you see a bunch of your friends sharing the same "watch out" post or you get direct messages telling you to copy and paste and send to all your contacts, stop. Please. Just stop.

Before you share, do a quick google search to see if there's a known scam going on. Don't perpetuate it.

23. …or stupid quizzes on social media – seriously, is it worth the risk?

Popular Facebook quizzes often ask users to answer a series of sharable personal questions, ranging from the name of their pet to their birth city. Some people see them as a fun way to bond with friends, or a way to make new ones.

The posts usually ask who was your first grade teacher, who was your childhood best friend, your first car, the place where you were born, your favorite place, your first pet, where did you go on your first flight …

But many of these queries are similar—if not identical—to security questions used by banks and other institutions.

So, you are giving out the answers to your security questions without realizing it.

In order to take certain quizzes or play certain games, you often have to give up access to your profile, your friends list, email address, and your birthday. Application hackers can then use any of that information to steal your identity or go and try to compromise an email or bank account.

Don't ever share your date of birth, mother's maiden name, first pet's name, or other personal information on websites like Facebook, LinkedIn, or Twitter.

Seriously, is taking a silly quiz really worth the risk?

24. Be conscious of unusual device performance

How do you know if you've been infected with malware?

Slow computing, unexpected behaviors like your laptop fan going on for no reason and for extended periods of time, excessive pop-ups and frequent crashes can all be signs of malware. If you are experiencing any of the above symptoms, it may be the result of malware symptoms that have gone undetected on your system.

Malware in action can consume a substantial amount of your computer's memory, leaving limited resources for other legitimate programs to use.

Threats such as spyware and computer viruses may be at work, tracking your activities, tampering with your files and stealing personal information.

So, be aware of unusual performance of your computer, laptop, or other connected devices and get it checked out.

Always turn off your computer at the end of the day – or if you prefer to just have it go into "sleep mode" without completely powering down, at least turn off the Wi-Fi connection. Idle connected devices are attractive prey.

25. THINK before sharing

Whether you know it or not, unless you are using a VPN, almost every action you take online is recorded digitally. Facebook, YouTube, Amazon -- to name a few — all use algorithms to track their users' online behavior. These companies then use this data themselves, or sell it on to third parties like advertising agencies.

I always tell my clients that you can't find what isn't there. Which means, if you're not foolish enough to share sensitive information, you won't have to worry about it being found and being used to hurt you.

That goes for compromising photos or controversial comments. We've all witnessed how some public figures – celebrities or government officials – have had their data exposed and sometimes used against them. You may never run for office, but chances are you'll probably look for another job at some point. So, don't be stupid about what you share online.

Use your common sense. You are what you share. Assume whatever you share can and will be used to target you – whether it be for unwanted advertising and communications – or for malicious intentions – by hackers, an ex-wife or ex-boyfriend, disgruntled employee or by anyone else.

You get the picture.

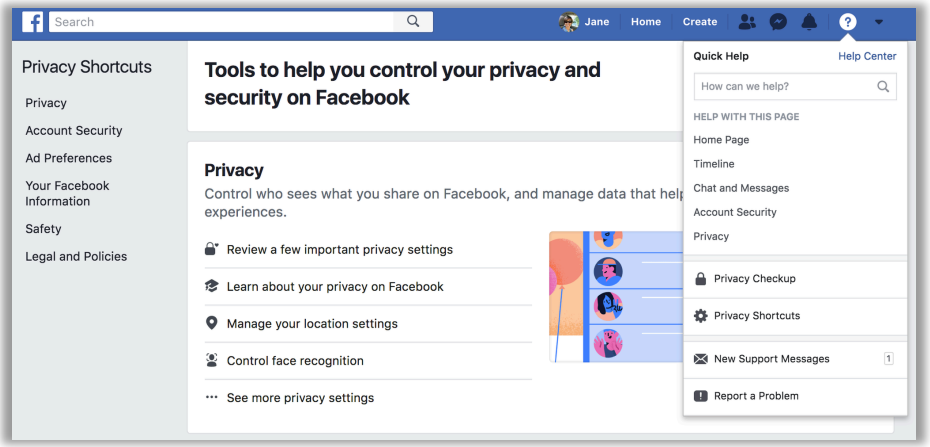
Enough said.

26. Actively manage your privacy and security settings on social media

Every safety precaution I've reviewed with you today so far is within your control – and really, pretty easy – if you just follow through.

One very important precaution to take is to actively manage your privacy settings in social media. You can't prevent Facebook, as a company, from getting hacked, but you can take measures to protect your privacy and security from random hackers from within Facebook's settings. You should make it a habit to review them every month or so to be sure that nothing has changed without your knowledge – or permission.

In Facebook, click on the question mark for Help & Support and go through the various settings.



26. Buckle up, here comes the Internet of Things

I've just shared the common threats and precautions to help you be safer TODAY.

But things are changing quickly. How do you prepare for the future and from new threats you don't know about yet?

The Internet of Things – or IoT for short - is just around the corner. And with this massive explosion in connectedness, the Internet will grow arms and legs.

What does that mean? Well, whereas current internet enabled threats normally attack data, information, our privacy – new IoT technologies will enable more vulnerabilities in the physical world – like in our cars, appliances, and yes, even sensitive medical devices. Because almost everything that CAN be connected to the Internet WILL be connected – whether it should be connected or not.

I've heard that there are new electric toothbrushes that will capture data on how well you're brushing your teeth. C'mon, do you actually NEED that??

Just because something CAN be connected, doesn't mean it should be.

So be cautious about embracing some of the new connected capabilities…because many IoT devices are easy to exploit. Manufacturers just aren't devoting enough resources to secure them.

It might be cool that your hip new "smart" refrigerator can sense when you're out of milk and notify you – or even order more for you from your grocery store. You THINK that the refrigerator data is harmless information that can't be used against you. But what if a hacker gains access and knows that your refrigerator door hasn't opened in 3 days? That probably means you're not home – which is just an invitation for a nice easy burglary.

Buckle up folks, this is the not-so-distant future that awaits us.

The most common exploit strategy is to simply attempt to connect to an IoT device using its default username and password. Whenever possible, change the password on your routers, smart TVs, and home entertainment systems. A lot of times, the default passwords are the same as Kanye's iphone password – 6 zeros.

When purchasing a connected car, carefully review and change its default security settings and avoid app installs from unknown sources. In addition, review the security and credentials of bluetooth connected devices, especially those that interface with your car's network.

I could spend an entire webinar JUST on the Internet of Things – and maybe someday I will – and I promise that everyone that attends this webinar will be the first to know if and when I do.

But suffice to say, with the internet of things (IoT) playing an increasingly significant role in our cars, homes, hospitals, even fridges, the average person is sharing a lot more data than they might think.

So, in what different ways are we sharing data, without even realizing it?

Here's an example that blew my mind – one that none of us would want to experience:

When you think of wearable fitness trackers, you think of a helpful device that helps you stay active – for example, by recording the number of steps you take in a day. Right? Well, in 2011, Fitbit users discovered that their sexual activity appeared in Google search results. OMG, that's just crazy.

I'm guessing that those users did NOT want that information tracked – and even worse, SHARED publicly.

Be proactive in learning more about data collection for any connected "thing" you buy or engage with.

27. If you become a victim of identity theft

In the unfortunate event that you become a victim of Identity Theft or some other security breach, there are some immediate steps you should take.

Make sure you change your passwords for all online accounts. When changing your password, make it a long one with the tips I already reviewed. You may also need to contact your bank and other financial institutions to freeze your accounts so that the attacker is not able to access your financial resources.

Close any unauthorized or compromised credit card accounts. Inform the card companies that someone may be using your identity, and find out if there have been any unauthorized transactions.

Think about what other personal information may be at risk. You may need to contact other agencies depending on the type of theft. For example, if a thief has access to your Social Security number, contact the Social Security Administration.

File a report with your local law enforcement agency. Even if your local police department or sheriff's office doesn't have jurisdiction over the crime, you will need to provide a copy of the law enforcement report to your banks, creditors, other businesses involved.

If your personal information has been stolen through a corporate data breach, you will likely be contacted by the business or agency whose data was compromised with additional instructions as appropriate.

If stolen money or identity is involved, contact one of the three credit bureaus to report the crime. Request that the credit bureau place a fraud alert on your credit report to prevent any further fraudulent activity from occurring - like opening an account with your identification. As soon as one of the bureaus issues a fraud alert, the other two bureaus are automatically notified.

For more tips, go to identitytheft.gov

I know I've shared lots of information with you today. You may have taken some notes, and I hope you did – because it may help you better retain this information take ACTION.

If you'd like to download a transcript of this webinar, click the button that just showed up on the right side of your screen. This download offer and link will only be available until the end of the webinar – when the countdown clock runs out.

28. Your personal data is valuable; Protect it like MONEY.

I don't think I really need to say anything else here except the words on the screen.

Your personal data is valuable. Protect it like MONEY.

I'm going to repeat this, just because after all I've reviewed here today, I really, really want it to sink in.

Your personal data is valuable. Protect it like MONEY.

29. What will you do differently today to be safer online?

I tried to give you a flavor for what the threats are and some steps you can take, some very simple and based on common sense. They'll make you safer and allow you to enjoy your connected time more – but they are UTTERLY useless unless you take them to heart and implement them. I hope you will.

Summarizing what we reviewed in this webinar, here are 7 things you can do or start doing today, right after you disconnect from this webinar. You still have time to get the transcript of this webinar to make your action items easier to remember…

Here they are:

1. Create strong passwords – or better, “pass sentences.”
2. Enable two-factor authentication.
3. Keep all software updated.
4. Back up important files.
5. Curb public Wi Fi use or get a VPN.
6. Manage your privacy settings in social media.
7. **Most importantly….Stop and think before you share or click.**

30. Cyber safety is everyone’s responsibility

The internet is vital to our economy and daily lives.

And as a result of this webinar, I hope you realize that protecting our digital lives is a shared responsibility. We’re all connected – and actions made by one can have impact on others – you can either be putting others at more risk by mistakes you make, or you can be making others safer by being diligent about your own online safety.

The more you know, hopefully the more you realize how important it is to take precautionary actions like the ones I shared here.

As I mentioned at the start of this webinar, my company, Scandurra Group, is proud to be an official partner of Stop.Think.Connect, the global online safety awareness and education campaign from the National Cyber Security Alliance. We join hundreds of organizations around the world in support of a safer, more secure and more trusted Internet.

I invite you to learn more about the mission of the National Cyber Security Alliance and the wealth of FREE cyber safety information they provide by visiting **staysafeonline.org**

31. Maximize Yourself. Connect with us.

I also invite you to connect with me and learn more about my business, Scandurra Group, and how I can help you and your organization thrive in the attention economy with winning strategies and solutions. This webinar is part of the Maximize Me Learning Series, with new webinars and courses added all the time. Everything is designed to help you thrive in the new attention economy.

So, that's it. I know it was a lot of information. I hope this webinar was helpful and that you'll put what you've learned into action. Start by downloading the webinar transcript before you log off this webinar – that's when the download offer ends.

You dedicated almost an hour of your life today to learn about good cyber safety practices. Make sure it was time well spent by motivating yourself to take action.

In fact, commit to implementing just ONE thing you learned today – right now, after this webinar – before you do anything else. Take that first step in empowering yourself to protect your valuable digital life.

Thank you so much for your time today. Bye for now!

Scandurra Group

Visit us at: SCANDURRAGROUP.COM

Practice cyber safety. Keep learning. Share the knowledge.

STOP | THINK | CONNECT™

Scandurra Group is proud to be an official partner of STOP. THINK. CONNECT.™, the global online safety awareness and education campaign. Scandurra Group joins hundreds of organizations around the world in support of a safer, more secure and more trusted internet.

Knowledge is Power

As cyber threats become more pervasive and complex, so do the resources needed to raise awareness on how best to thwart them. Most people are fully aware of the need for better protection, but lack a sense of urgency to take steps to safeguard themselves - until it's too late.

Scandurra Group is dedicated to offering cyber awareness education, sharing best practices to help protect the digital lives of individuals in our tech-fueled, socially connected, attention economy.

maximize
LEARNING SERIES
POWERED BY SCANDURRA GROUP

Capture and Hold the Attention of Others:

Cutting through clutter has become much harder as the amount of choices and level of mass distraction has grown. How do you capture and leverage the precious attention of clients, prospects, employees and influencers? Adopt effective strategies and tactics that build credibility and trust and demonstrate your unique value as an individual or an organization. Stand out from your competition, drive new opportunity and influence lasting success.
Learn more: ~ Personal Branding ~ Social Media Enablement

marketing effectiveness

motivated ecosystem

meaningful engagement

Harness and Channel Our Own Attention:

In a distracted world where multi-tasking is the norm, our inability to focus has become a conditioned state - an unintended consequence of our connected world. As a result, innovation, productivity, health and relationships suffer. Get back on track. Become a lifelong learner and ensure you maximize your skills to stay relevant in a changing job market. Regain and reinforce critical, uniquely human traits that will prove invaluable in the future of work. Learn to focus on developing the habits necessary to enjoy a healthy and happy modern lifestyle.

mindset & energy

modern employment

more education

*"Tell me what you **pay attention** to, and I'll tell you **who you are**."*

-Jose Ortega y Gasset