9 CYBERSECURITY TIPS FOR EVERYONE

Education Center

Powered By BankersTrust

In today's digital world, we live a life immersed in technology. It has become part of our culture and has revolutionized our perspective of the world while fundamentally altering the methods we use to stay informed with breaking news, interact with our loved ones, stay up-to-date with friends and even complete our banking needs.

As with most new developments and innovations, there are risks involved in using technology. Throughout this guide, we will provide tips on how you can stay as safe as possible while in cyberspace.

TABLE OF CONTENTS

CHAPTER ONE

The Dangers of Public Wi-Fi

In this day and age, people are looking for ways to stay connected to friends and family and everything else the internet has to offer. In order to constantly stay connected, users often need access to public Wi-Fi.

Across the U.S. and most other places in the world, you can find a place to connect on almost every corner, including in places like airports, coffee shops and hair salons. With such easy access to public Wi-Fi wherever we go, we shouldn't have to worry about getting on the internet anywhere, right? Wrong! Public Wi-Fi is extremely dangerous. Here's why.

Why public Wi-Fi can be risky

While connected to a public Wi-Fi network – like one at a coffee shop, for example – any other computers also connected to the public network can reach your computer and attempt to break into it using a number of potential vulnerabilities.

And that's just the beginning. A hacker connected to the same network can also:

- **Trick your computer or phone into thinking their computer is the Wi-Fi router,** making your device send all traffic to the malicious computer before it gets out to the internet. All your unencrypted information can now be seen and stolen by the hacker.
- **Set up a fake website that looks and acts exactly like a real website you want to visit**. While you think you're seeing the real site, you're actually visiting the hacker's spoofed site. You type in your password to a site, and just like that, the hacker has your credentials and can log in as you.
- **Set up their own real Wi-Fi access point**, set the name to something that seems legitimate, or even the same name as an existing Wi-Fi network, and then perform the same attacks mentioned above with even greater ease.

So what can we do to protect ourselves from the dangers of public Wi-Fi? **The most obvious solution is to not use public Wi-Fi and to use your mobile data or hotspot from your phone to your laptop instead.** However, if this is not a viable option because of data costs, consider the following tips for situations when you must use Wi-Fi:

Avoid obviously bad Wi-Fi Points

Wi-Fi access points with names like "Totally Free Wi-Fi" are probably not safe. However, even a legitimate-sounding Wi-Fi name can be dangerous.

Only use sites that use HTTPS

HTTPS encrypts the traffic to the website while HTTP does not. Although this will protect us most of the time, not all websites are properly configured and some only use HTTPS on specific portions of their sites.

Secure your computer and phone

A hacker may try to break into your machine using some vulnerability. One way to reduce your computer's vulnerabilities is to keep the operating system and anti-virus up-to-date. Always install all updates and disable sharing services on your computer while using public Wi-Fi.

Use a VPN whenever possible

Using a good VPN is the best way to ensure all your traffic is encrypted and secure when on public Wi-Fi. You can do a quick online search to find the top-rated VPN solutions. The best offerings have Android, iPhone, and computer versions, and they are also not free.

If you must use public Wi-Fi, avoid using financial sites or sending personally identifiable information (PII), such as your social security number, driver's license number or passport number. This is information you definitely don't want stolen, so it's better to be safe than sorry.

CHAPTER TWO

The Strength of Your Passwords Matter

Are you using the same password or email address for all of your online accounts? It's understandable if you are, given the increasing number of online accounts we're expected to manage today. However, in today's digital world, nearly everything is online, and it's your responsibility to protect your personal information and financial accounts from cyber criminals.

In order to protect your information, it's essential to use unique, strong passwords for important accounts, as well as a separate email address to register and manage accounts when possible, especially for your email and any finance- or health-related accounts.

Here's one example of how a hacker could gain access to your online accounts:

- You use the same email address to register all of your online accounts (e.g. social media, banking, and retirement accounts).
- A hacker gains access to your email account and is able to quickly identify where you bank, what credit cards you have, and where your retirement accounts are managed.
- The hacker attempts to log onto your online accounts using the password he already knows.
- After a number of failed log on attempts, the hacker is prompted to reset your password by emailing a temporary 'Password Reset' link to the registered email account. Or, he could easily click on the "Forgot Your Password" link and have the link emailed to the registered email account, to which he already has access.
- The hacker clicks on the link, resets your password and deletes the email so you're not aware of the change.
- The hacker now has full access to your online accounts.

Sounds scary, right? This is just one example of why you need a strong password, but there are many more. On the next page, learn how to create a strong password.

How to create a strong password

- **Password length:** Use a minimum of 12 characters; the longer the password, the better.
- **Complexity:** Use capital letters, lower-case letters, symbols and numbers.
- **Don't use full words or names in your password** (e.g. Happy21, Shannon1982).
- **Don't rely on substitutions to replace letters with numbers or symbols** to try to pad words (e.g. H@ppyB1rthday).
- **Use a phrase that's easy to remember, and create your own algorithm** to encrypt the phrase. For example: Your personal algorithm may be to use the first two letters of each word in your phrase with the first letter being capitalized for each word, replacing words with symbols and numbers when possible, such as:
    - Phrase: **Follow The Yellow Brick Road To Get Money**
    - Password: **FoThYeBrRo2Ge$**

Now that you know what a strong password looks like, you can start using them across your online accounts.

Creating a variety of strong passwords might make it hard to remember them all, which is why we suggest also using an online password manager.

CHAPTER THREE

The Importance of Software Updates

Another day, another pop-up window on your computer asking you to re-install, update, or download some new software. What a nuisance, right? Well, maybe not. Security issues are some of the most aggressive and tenacious threats and those software updates can be critical when it comes to protecting your device from viruses and hackers. After creating a strong password, the next step is to update your security software.

Imagine the following scenario:

You unknowingly visit a website that has been hijacked by a malicious attacker. Even with a brief visit, the website can scan your computer for security software that has not been installed or updated. The hacker then attacks those vunerabilities with malicious code. Suddenly, software called a rootkit is installed on your computer that can "hide in plain sight" any viruses and malware, making it close to impossible for any other antivirus software to detect. Next, a Trojan downloader begins firing off processes to download additional malware to your system. This is only the beginning...

How do you minimize the risk?

Regularly installing updates helps safeguard your software, as hackers target those who are late to update to the newest security measures. Keeping any other anti-software you have up-to-date is also critical. Anti-software companies create updates to correct bugs in your computer's existing software and sometimes also provide minor functionality improvements. You can opt to either have your updates install automatically or elect to install them yourself at a time most convenient for you. Either way, make sure you stay on top of those updates.

Installing reliable anti-virus protection on your devices goes a long way in protecting against malicious software that can corrupt your system and destroy or steal your data. Keep in mind, simply installing anti-virus protection is not enough to prevent malware. Staying on top of updates is what will make a difference in protecting your privacy.

Be cautious of free apps

Be cautious of free applications and research them before you download. A quick search should help you find out if the free app you are interested in is reputable and free of malware.

Change default credentials

Many of your home devices, such as your wireless router/modem combo, will come with default login credentials. These credentials are widely known, so change the password as soon as you receive the device to prevent unauthorized and malicious access.

CHAPTER FOUR

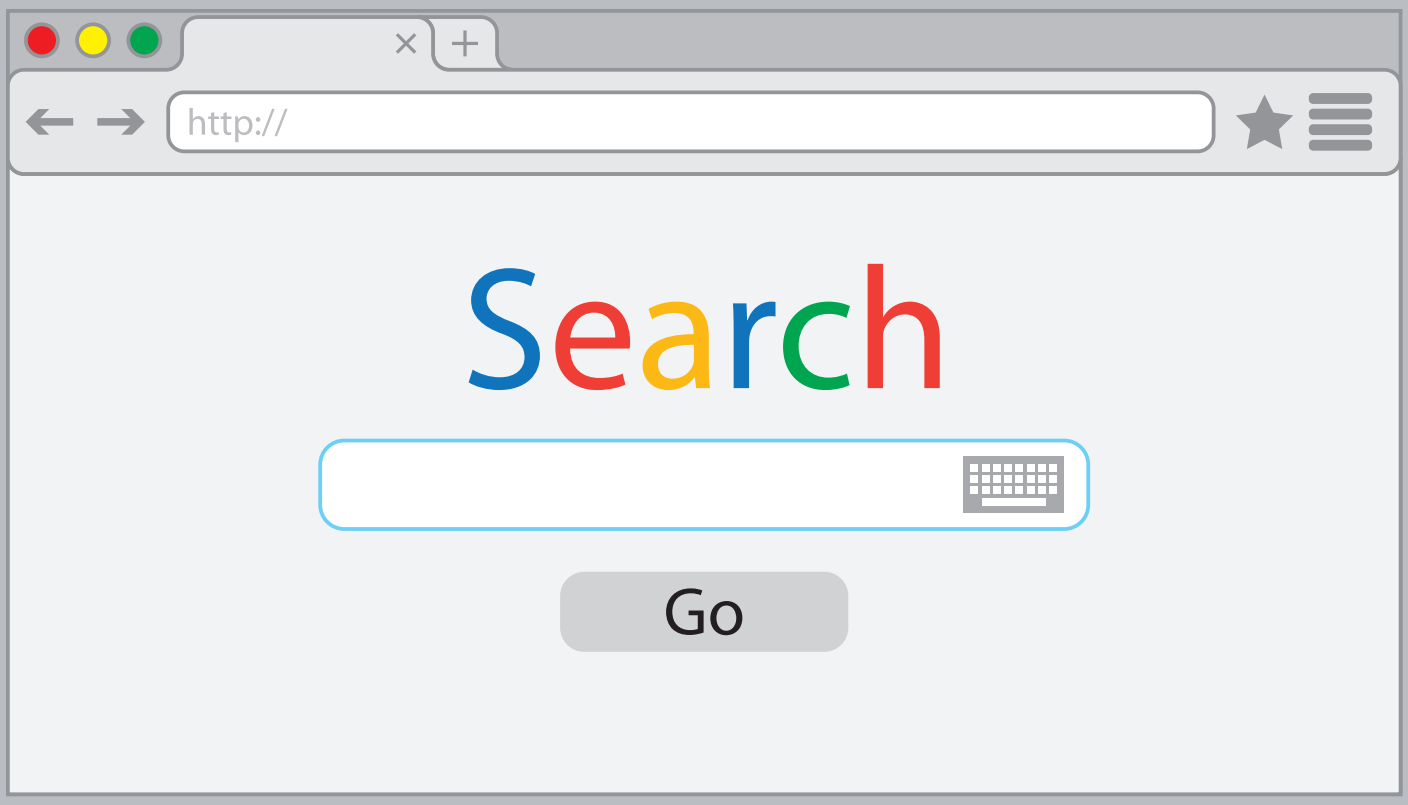
Getting to a Website the Right Way

Software updates, anti-virus protection and strong passwords are all crucial steps to take to protect your online identity. But did you know the way you type in a URL can also make a difference in your cybersecurity?

The best way to safely find your way to a website is to use a search engine.

It is common to type a URL directly into the address bar to get to a website. This is becoming more risky, as a simple misspelling can direct you to a malicious website that's designed to look like the site you're trying to visit. Just seconds on that site could spell disaster.

To be safe, search for the website you want to visit using your favorite search engine, and use the links in the results to reach your destination. Then save the legitimate link in a bookmark to click on later without fear of misspellings.



CHAPTER FIVE
Social Media Safety

People all around the world spend a significant amount of time online using a variety of social media platforms including Facebook, Instagram, Twitter, LinkedIn, Pinterest, and YouTube. We *google,* we *tweet,* we *like,* we *skype,* we *post,* we *tag,* we *check-in,* we *engage*. While social media can be an amazing resource that allows you to connect with friends and family, it can also greatly increase privacy risks.

For example, companies are storing large amounts of data about each of us. The most obvious is data being collected from social media. Everything we post publically, and even privately, is stored and analyzed.

And it's not just social media. There is now a digital record of everything you purchase, everything you watch, and everywhere you go online. All of this data is used to create consumer profiles. Using unique algorithms, companies use this information to cater marketing strategies directly toward your unique preferences.

Some groups even profile you to specially adapt their interaction with you, whether it's an email or social media ad. The aggregation and storage of this data is becoming one of the most profitable enterprises on the planet.

Everything you do on social media can be collected. Even after social media accounts are deleted, personal information can still be collected from a variety of online sources.

Before posting online, think about these three simple questions:

- Am I OK with this post existing forever?
- Am I OK with this post being read by anyone?
- Am I OK with this post being used to profile who I am?

If the answer to these questions is yes, post away. If the answer is no, reconsider what and how much you want to share online. Just remember that the information is always out there.

CHAPTER SIX
Phishing

Would you willingly give your password or other private information to a stranger? Of course not. Let's say that you receive a 'Suspicious Account Activity' email from a financial institution asking you to log in to your online account and verify a transaction. Would you log in using the provided button or link in the email? If so, you may be putting yourself at risk of falling victim to a phishing attack.

Phishing is the attempt to obtain sensitive information such as usernames, passwords and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Why would someone target you in a phishing attempt? Cybercriminals know where the money is. That's why they commonly use financial institutions when targeting individuals. Criminals use deception to manipulate users into providing them with valuable login credentials or other PII.

Phishing scams aren't limited to email

A quick phone call is an easy way for a criminal to build trust and catch people off guard. New internet phone technologies make it easier than ever for cybercriminals to hide their actions from law enforcement.

Think about this. Have you ever been to a restaurant and left a copy of your receipt on the table? Or left that gas receipt in the gas pump? Believe it or not, that receipt has a lot of private information on it. This information can be used against you to make you believe that a threat is real. These criminals are professionals at what they do, and the quicker they gain your trust, the more dangerous they become.

The next time you go shopping, look at your receipt. You will find your full name, the last 4 digits of your credit card number, time of visit, place of transaction, and what was purchased. On the next page, see how a cybercriminal could use this information:

A criminal is sitting at the table across from you and sees the name of the bank on your payment card. As you're walking away, she quickly gets up and grabs a copy of the receipt off of the table. She pulls out his phone and does a quick social media search using the name on the receipt. She's able to find where you work, your contact information, and cell phone number within minutes. The criminal immediately starts putting together a targeted phishing attack. The following morning, you are running errands and the phone rings. You answer the call and have the following conversation with the cybercriminal:

You: Hello.

Phisher: Good Morning. This is Susan calling from Your Local Bank Anti-Fraud Department. Am I speaking with Lucas Freeze?

You: Yes, this is Lucas.

Phisher: Mr. Freeze, I'm calling you today because our fraud protection system alerted us about some fraudulent activity on account ending in 1234. Is that your card?

You: Yes, it is.

Phisher: I'm going to ask you a few questions to confirm your identity and verify these transactions. Can you please confirm your home address?

You: 12345 Memory Lane, Secure Town, IA 55555

Phisher: Thank you. Are you currently employed at ABC Company?

You: Yes.

Phisher: Mr. Freeze, did you recently complete a transaction at Fake Event Tickets for $494.89?

You: NO!

Phisher: Okay, Mr. Freeze, how about a transaction for $49.89 at Fresh Seafood – Nothing Better?

You: Yes, that was me.

Phisher: Mr. Freeze, I think your card has been compromised. I would like to suggest that we cancel your card immediately. Would you like to go ahead and process the cancellation?

You: Yes, please.

Phisher: Mr. Freeze, can you please confirm the remaining digits on the card so I can be sure we're cancelling the correct card? The name on the card is Lucas M Freeze, correct?

You: Yes.

Phisher: Okay, Mr. Freeze, please go ahead and provide me with the complete card number.

You: 1234 5678 9123 4567

Phisher: Thank you, Mr. Freeze. That matches the card we have on file. Can you please confirm the expiration date and three-digit code on the back of the card?

You: 01/20 and 123.

Phisher: Thank you, Mr. Freeze. I have processed the cancellation and ordered a new card for you. Please allow 7-10 business days for your new card to arrive. I also put the transaction for Fake Event Tickets, in the amount of $494.89, into dispute which will remove the transaction from your account immediately. Do you have any questions?

You: No. Thank you for catching this so soon.

This is one example of how professional cybercriminals can get your information over the phone.

You should never provide personal information, credit card numbers, Social Security numbers, or any other non-public personal information to anyone if you did not initiate the communication.

CHAPTER SEVEN

Mobile Deposits

While mobile deposits are a convenient way to deposit your payroll or personal checks anytime and from anywhere, there are a few things you should keep in mind to prevent becoming a victim of a mobile deposit scam.

What is mobile deposit?

Mobile banking apps with a mobile deposit feature can save you a trip to the bank and allow you to deposit checks whenever is most convenient for you. Just take a picture of the front and back of the check and upload!

How does a mobile deposit scam work?

Fraudsters contact their victims through email or social media posing as a potential employer, lender, or interested buyer on a marketplace site. The fraudster will often provide the victim an opportunity to earn money quickly by depositing a check to their account or by asking for help in moving money from overseas. The fraudster will further request the victim's bank account information and may even ask for online or mobile banking login credentials.

The fraudster uses the information to deposit a fake check. Once the deposit has been made, the scammer will request funds to be immediately transferred back to them via money order, person to person transfer, wire transfer, reloadable cards or even gift cards. Once the victim returns the funds, the bank alerts the victim that the check was fictitious and removes the funds from the account, causing a loss to the victim.

How do you protect yourself?

Never give out your personal information to people you don't know, alert your bank of any suspicious activity, and before you deposit a check, look for these red flags:

- Typos in names of the payer, payee, bank and dollar amounts
- Out of state payers and out of state banks
- Missing or faded bank logos
- Notations in the memo-line suggesting legitimacy (cash, authorization, void after 30 days, payment, etc.)

And remember, even if a check has been "cleared," you may not be in the clear. Under federal law, banks must make deposited funds available quickly, but just because you can withdraw the money doesn't mean the check is valid, even if it's a cashier's check or money order.

If you have any questions about whether or not a check is valid, talk to your banker.

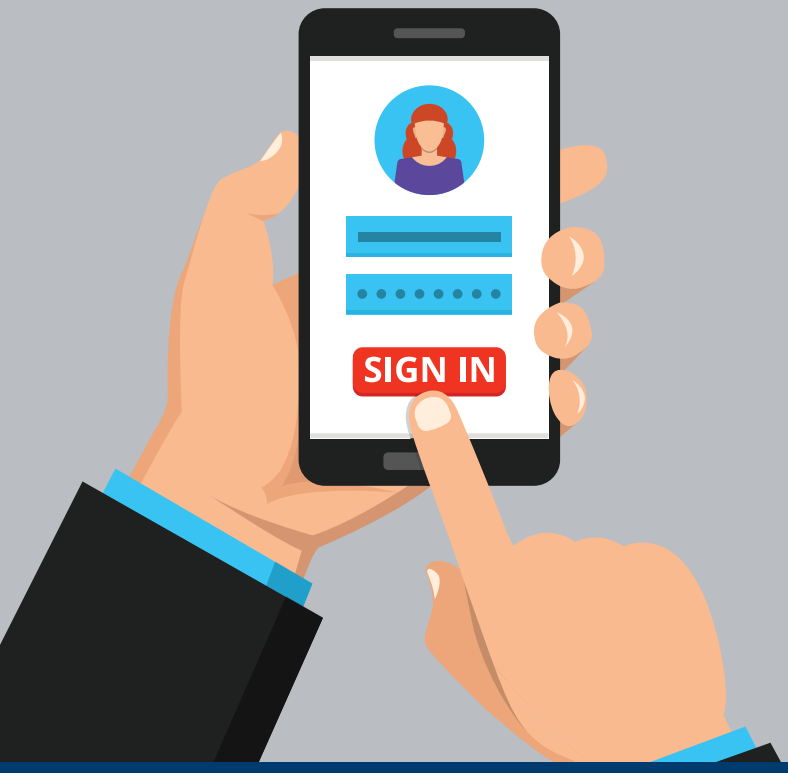
CHAPTER EIGHT

Port-Out Scams

Did you know your cell phone number can be stolen, along with your money and identity?

A port-out scam is a way for hackers to steal your hard earned money and even your identity by taking control of your cell phone number and your phone service. The scariest part is that this type of scam can also help scammers get past added security measures on personal and financial accounts. However, you can keep yourself protected by taking simple precautions.

Port-out scams have been trending across the country. Cell phone porting involves a scammer finding your name and phone number and attempting to gather your PII. This may include your Social Security number, date of birth, or other information that can be used to steal your identity. The criminal will then contact your cell phone provider impersonating you, and inform them that your phone was stolen and request for the number to be "ported" with another provider and device.



Once your number is ported, they can start accessing and entering accounts that require additional authorization, such as a code texted directly to your phone. These added security measures are usually provided by social networks, tax preparation software, email providers, and financial institutions.

Think of how many times you have set up an account for social networking, email, or your online bank account. Or maybe you had to change your password—how many times were you required to verify your identity through a text message code? What if you weren't the only one who was reading that message? The port-out scam could bypass that layer of security and steal your identity faster than you think.

Protect yourself from port-out scams with these tips:

1. **Inquire with your wireless provider about port-out authorization.** Most major wireless companies have additional security for accounts that customers can set up, such as a unique PIN or added verification question.
2. **Call your mobile phone company if your phone suddenly switches to "emergency call service only" or something similar.** This can happen when your phone is being transferred to another phone and will only allow you to make emergency calls.
3. **Be cautious about communications you receive.** Watch for alert messages and texts in response to two-factor authentication requests.

CHAPTER NINE

What You Should Do If You Think You've Been Hacked

Some of us have been there. You notice unfamiliar transactions on your bank statements. You read sent messages you don't remember sending. You can't access your account despite using the correct password. Your computer is running slower, and your anti-virus protection is disabled. There are software add-ons on your computer you don't remember downloading. These are all signs you may have been hacked.

What do I do if I think I've been hacked?
If you believe your internet banking account has been compromised, contact your bank immediately. The bank's financial intelligence team will replace compromised cards, reset passcodes, and get to the bottom of the attack. Here are a few other steps you should take:

- **Consider freezing your credit.** This will prevent unauthorized access to your credit, and you can lift the freeze any time.
- **Let your family and friends know you've been hacked.** If you've experienced email compromise, the hacker may reach out to your email contacts, so it's critical you warn them.
- **Change your passwords.** Make them tricky to crack by including symbols, numbers, and random characters.
- **Reinstall your anti-virus protection** and backup the data on your computer.
- **Continue closely watching** your financial accounts.

Here are red flags to look for if you suspect you've been hacked:

- The number calling you is not a local number. Keep in mind that a local number does not mean it's *not* a hacker, as they can make it look like the call is local even if it's not.
- The "representative" you're speaking to asks for your username and password. A legitimate bank employee will never ask for this information and will have different methods of verifying your identity.
- The message you receive or the "representative" you're speaking with rushes you into taking action.
- The message you receive includes grammatical errors or is poorly written.

Despite taking precautions, there are always security risks involved when using the internet. Being familiar with red flags and signs you've been hacked, you can take action quickly to limit the damage. Check your bank statements regularly, use strong passwords and use different passwords for your email, social media, financial and other accounts.

CHAPTER TEN

What's Next?

You can never be completely safe in cyberspace, but by taking certain precautions, you can greatly reduce your risk of falling victim to cybercriminals and become better prepared to respond to cybercrimes. Social media, online banking and the internet are convenient for keeping in touch with our friends, depositing checks from anywhere, looking up the answer to a random question, and so much more. However, these innovations also open the door to more risk. It's important to take precautions to limit risk as much as possible.

Key takeaways:

- Having a strong password is the first step in this process and can make a huge difference when it comes to your personal, financial or health-related information.
- Make sure that your anti-virus software is up to date on both your computer and phone.
- Try to avoid using public Wi-Fi
- Don't give out personal information to anyone you don't know.
- Stay up to date on the different types of popular scams. Knowing how to limit risk is the first step in a protecting yourself in cyberspace.

Stay up-to-date on the latest security issues and tips by subscribing to weekly emails at Education.BankersTrust.com.