Brought to you by:

thycotic

Cybersecurity

for dummies®

A Wiley Brand

Recognize top cybersecurity threats

Respond to a cyberattack

Protect yourself at work and home

Joseph Carson, CISSP

Thycotic Special Edition

About Thycotic

Thycotic, a global leader in IT security, is the fastest growing provider of Privileged Access Management (PAM) solutions that protect an organization's most valuable assets from cyberattacks and insider threats. Thycotic solutions enable organizations to improve cybersecurity by protecting passwords and account credentials, increasing productivity through automated controls, and demonstrating compliance with robust auditing, monitoring, and reporting capabilities.

Thycotic secures privileged account access for more than 7,500 organizations worldwide, including Fortune 500 enterprises. Thycotic's award-winning Privileged Management Security solutions minimize privileged credential risk, limit user privileges, and control applications on endpoints and servers. Thycotic was founded in 1996 with corporate headquarters in Washington, D.C. and global offices in the U.K. and Australia. For more information, please visit **www.thycotic.com.**

Cybersecurity

Thycotic Special Edition

by Joseph Carson, CISSP

for dummies®
A Wiley Brand

Cybersecurity For Dummies®, Thycotic Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-46735-9 (pbk); ISBN: 978-1-119-46739-7 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie A. Burchfield
Editorial Manager: Rev Mengle
Acquisitions Editor: Amy Fandrei
Business Development Representative: Ashley Barth

Introduction

The issues and challenges associated with *cybersecurity* — the measures taken to protect computer systems against unauthorized access or attack — come up almost daily in your work and home lives these days. Media headlines highlight the latest breaches of confidential information, exposing millions of personal information records. Executives lose their jobs because of these incidents. Companies sometimes see a sudden drop in their stock market value. Others must pay a "ransom" to get their hijacked information back. And for smaller organizations, their very existence as a business may be threatened.

Despite billions of dollars spent each year on sophisticated technology to help protect critical information assets, hackers and malicious insiders continue to steal information with seeming impunity. The vast majority of breaches in cybersecurity are the result of human errors or actions that often occur without people even being aware of what they have done.

Technology alone can't protect your identity or sensitive information. Hackers and other threat actors target humans, seeking ways to trick them into giving up vital information unknowingly. They do this because it's the easiest way to get at valuable data in a process known as *social engineering.* So, it's not surprising that exploited humans are the weakest link in the cybersecurity chain and yet the best hope for preventing a cybersecurity disaster.

About This Book

Cybersecurity For Dummies, Thycotic Special Edition, helps you understand and recognize the most common cybersecurity threats people face daily in their personal and work lives. With that understanding, you can then begin to adopt good cyber hygiene that helps you avoid becoming the next victim. Spending a few minutes reading this book also helps you learn how cybercriminals target their victims, what you can do to reduce your risk, and how you can personally make it much more difficult for the attackers to steal your information, your identity, and your money.

Icons Used in This Book

This book uses the following icons to indicate special content.

You don't want to forget this information. It's essential to gain a basic understanding of cybersecurity threats and how to detect them.

The Tip icon points out practical advice that saves you time and effort in improving your own cybersecurity hygiene, and this information also helps you avoid getting cyber fatigue and reduces your risk of being a victim of cybercrime.

Watch out! Pay close attention to these details. They focus on serious issues that have a major impact on you and your organization's security.

Beyond the Book

Because cybersecurity is literally everywhere in your always-on, Internet-connected lives, you need to get on board with recognizing that the more you learn about how to protect yourself, the easier and safer your life will be. But your learning can't stop with changing a few passwords or taking a few tips from this book. You should continually educate yourself.

Many online safety awareness campaigns exist that offer practical, up-to-date advice on how you can stay safer and more secure online. I recommend the following two:

- https://stopthinkconnect.org
- https://safeandsecureonline.org

IN THIS CHAPTER

- Targeting humans as the primary cause of breaches
- Fighting cyber fatigue

Chapter 1
Cybersecurity Is Everyone's Responsibility

In our always-connected world where the private information of individuals and organizations is vulnerable to exposure and misuse, cybersecurity is everyone's responsibility because hackers or malicious threat actors who steal proprietary information don't care about age, gender, race, culture, beliefs, or nationality. They probe your digital footprint and your Internet-connected computers based on opportunity, often seeking financial gain.

Targeting Humans

People are the number one target and cause of cybersecurity failures because most of them are trusting individuals who want to help or contribute as part of human nature and their jobs. Hackers and malicious insiders take advantage of that trust by appearing to make legitimate business requests from bosses or sharing social items of a more personalized nature. They're counting on people's curiosity and willingness to cooperate to get them to "click on the link" in a business or personal email.

WARNING

One single click on a malicious link, however, can download malware onto your computer that can immediately lock up data in a "ransomware" attack, and oftentimes, you have to send money to regain access. Or, the downloaded malware can, unknowingly to the user, begin instantly collecting information aimed at gaining credentials and passwords for exploiting later. While many of these actions by humans are accidental or not intended to be harmful, the result can cause considerable damage to themselves, their family, their co-workers, their company, and their community.

Hackers want to steal your identity and credentials

As the use of the Internet and social media have grown, hackers and cybercriminals have changed the techniques they use to target people. Email continues to be the number one weapon of choice, followed by infected websites, social media scams, and stealing digital identities and passwords.

Recent research shows that up to 80 percent of all data breaches involve compromising an employee's credentials. In one survey, hackers claim that stealing an employee's password is the fastest (and most preferred) way to breach and bypass a company's cybersecurity controls.

As you connect to online services to get the latest news, shop for the best deals, chat with friends, stream music and videos, and conduct banking transactions, you quickly become a target of cybercriminals. Using social media, for example, you typically share a lot of personal identifiable information about your physical and digital identities. This info includes full name, home address, telephone numbers, IP address, biometric details, location details, date of birth, birthplace, and info on other family members. Cybercriminals know this and can spend up to 90 percent of their time performing reconnaissance by using online social media sources to apply advanced search techniques and specialized search engine parameters to uncover confidential information from companies and individuals that doesn't typically show up during normal web searches.

Hackers are specifically looking to steal your username and password credentials so they can access your information and impersonate as you. And, when your identity is stolen, an attacker can easily bypass the traditional technical security perimeter controls without being detected. Once inside the computer network, cybercriminals can carry out malicious attacks or access and steal confidential information by posing as a legitimate user.

Your work and personal info are all linked in cyberspace

The protection of information about both your work and personal life can no longer be separated. The frequent and pervasive use of social media networks, working from home or when traveling, and the Internet of Things (IoT) connecting all kinds of household devices means that cybersecurity is no longer just the responsibility of your company IT department. A compromised personal account can easily lead a hacker to discover enough information about you to make hacking your business email so much easier.

REMEMBER

As the line between business and personal Internet use continues to blur, every employee must contribute in protecting information assets at work and at home.

Standing on the Frontline

Many folks at work and home suffer from *cyber fatigue,* which describes the frustration experienced in juggling scores of online accounts with multiple passwords needed to gain access to the information you use daily or hourly. In some cases, individuals feel so frustrated that they give up trying to manage things safely and default to using the same passwords for multiple accounts, sharing passwords with family members, and logging in to the Internet using their social media accounts.

REMEMBER

You are the frontline in the battle to keep information secure. Attacks rely on your goodwill and trust to succeed, so you must become more personally responsible in how you manage your information, and this can be tiring.

TIP

To overcome cyber fatigue (or to avoid it all together), I suggest following these tips:

- Simplify your logon experience by using a password manager that will help reduce the pain of selecting long complex passwords, remembering too many passwords, and choosing unique passwords for each account. A password manager will do this for you.
- Set your programs, applications, and security software to automatically update so you don't have to manually do it. One of the most important steps in cybersecurity is staying up to date, and enabling auto updates helps you so you don't have to worry about getting the latest security patches.
- Schedule data backups to ensure that when bad things happen you always have a solid backup to get back on track and not get stressed out about losing important data.
- Stay educated on the latest security trends so you know what's important and can help avoid information overload about not knowing what's happening in cyberspace.

IN THIS CHAPTER

- Identifying different email scams
- Looking at the risks in social media
- Checking activity logs, mobile usage, and bandwidth
- Being leery of public Wi-Fi

Chapter 2
Recognizing Top Cybersecurity Threats

Cybercriminals utilize an expanding set of online tools and services available with hacking as a service, distributed denial of service (DDoS), and the latest ransomware as a service. This means attackers no longer require any deep technical knowledge to carry out their attacks — they just need a laptop and an Internet connection. So you'll be targeted now more than ever, and you must be prepared.

Cybersecurity incidents are typically classified in three categories:

- Access or loss of sensitive or personal information — known as impacting confidentiality
- Possible modification of sensitive or personal information — known as compromising integrity
- Destruction or loss of availability to sensitive or personal information — known as reducing availability

The type of cyber incident determines what actions and steps should be taken to minimize the impact or damage from the incident.

In this chapter, I give you techniques to identify the main cybersecurity threats. In Chapter 3, I tell you how to respond.

Ransomware

If you have a ransomware attack, you know almost immediately because you see a message from the cybercriminal that your files have been encrypted or that you have been locked out of your computer. Note that it's common to see mistakes in spelling and formatting in these types of messages. This message can look similar to Figure 2-1. You will then be asked to pay a ransom to get an encryption key and restore your files. Payment is typically demanded in Bitcoins or some other well-known cryptocurrency.

FIGURE 2-1: A typical ransomware message.

WARNING

If you see such a message, it's vital that you make sure it doesn't spread to other devices at work or at home. Disconnect the infected computer from the Internet or your company network. Remove the network cable, turn off Wi-Fi, and power off your device. If it occurs on a company computer or occurs on your company's network, immediately notify your IT department.

Email Threats

Email continues to be the most popular weapon of choice when it comes to stealing credentials, installing malware, or locking up information in a ransomware attack. Hackers prefer email because all it takes is for one victim to open an attachment in an email or click on a link to open the door for attackers to exploit.

Spam emails

Spam emails show some personal information and can look very authentic so you must examine them *all* carefully. While spam filter technologies do a better job at screening threats, spammers are getting better at incorporating authentic details, including already disclosed or stolen personal information, that enable them to get through into your email inbox.

One simple method used by hackers to capture information about what device and browser you use, software versions, patch levels, and more features an HTML email sent to you with a tiny image similar to the example in Figure 2-2. Simply clicking on this email will download the image automatically into your email client by default unless you change your settings. And in downloading that image you share information that hackers can use to exploit your systems.

TIP

To prevent sharing information about your device and location, make sure to disable automatic image downloads in your email client. That way you control when to download images from incoming email.

FIGURE 2-2: An example warning message when image is included.

Phishing emails

Phishing emails often contain personal information and can be very authentic looking, typically pretending to be a legitimate service from a known vendor. Phishing emails almost always pose as an urgent message from an authority that requires a quick action, such as clicking a link or opening an attached file to avoid further trouble, late fees, and so on. These emails normally contain multiple hyperlinks — some are legitimate to disguise the one malicious link among them. You can see an example of this type of email in Figure 2-3.

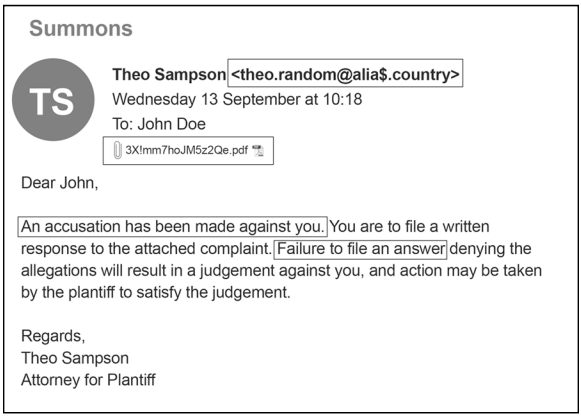

FIGURE 2-3: A phishing email example with highlighted indicators of threats.

WARNING

Do *not* open or click on any suspicious link or attachment because this could corrupt your system and give cybercriminals access to all your data.

Cybercriminals intelligently comb through public social data, searching for victims that are easy targets and will yield the quickest access. They collect info to form a digital footprint of potential victims, hoping they will be tricked into revealing more sensitive information including account passwords, access to email, or even full control of devices.

WARNING

Watch out if the email display name doesn't match the email address of the sender or if the attachment has a random sounding name, or if the hyperlink display names don't match the actual URL of the attachment. Simply hover your mouse over the link to reveal the real URL address, but *do not* click the link. These threats are also becoming more popular on social media and messaging applications that are very difficult to tell the difference — sometimes only containing a single character difference — so watch out for these threats via messenger applications.

TIP

Just like with known spam, mark the senders of your suspected phishing emails as junk or spam, and report them immediately to your IT Security department if they appear directly in your work inbox. Don't forward a phishing email. Make sure you've taken basic steps to protect your devices and scanned your system and emails for malware.

Spear phishing emails

Spear phishing emails target you personally, pretending to be from someone you know and trust, such as a friend, colleague, or boss. They contain a hyperlink or attachment, such as a PDF, Word document, Excel spreadsheet, or PowerPoint presentation.


WARNING

The most frequent spear phishing attacks appear to come from your employer's executive management team or someone in authority requesting you to perform an important action — either opening an attachment or in some cases an urgent transfer of money to a link in the email.


TIP

Limit what you share on social media, and enable privacy and security settings on your Facebook, Twitter, or other social accounts. Don't accept "friend" requests unless you know the person well.

Social Media Threats

Social media and their associated social usernames and passwords have become part of everyday life. While email is still the preferred tool for cybercriminals, social media has become more popular because when you create social media accounts, you open the details of your life to cybercriminals searching for personal information. Social media accounts continuously ask you to provide more details about your date of birth, location, phone number(s), workplace, education, home town, and family members. They want this information to target you for personalized feeds, custom preferences, and advertisements and to help connect you with people, events, or groups that fit your interests.


TIP

On social media, limit your Personal Identifiable Information (PII), which is information such as your mobile number or home address. Whenever using or creating a new social media account, only enter the basic information required to get the account activated. Avoid the temptation to add more details. If you've already added this information, change your settings to hidden/private or remove them from your profile.

WARNING

As you create more online accounts, social media accounts offer themselves as a single sign on, as shown in Figure 2-4, to simplify and reduce the ever-growing cyber fatigue of remembering passwords, but such convenience disguises huge risks. If your social media account is compromised, a cybercriminal can easily access all your other associated accounts by using that *one* social media account password. Instead of using social logon, consider using a password manager (details in Chapter 4).

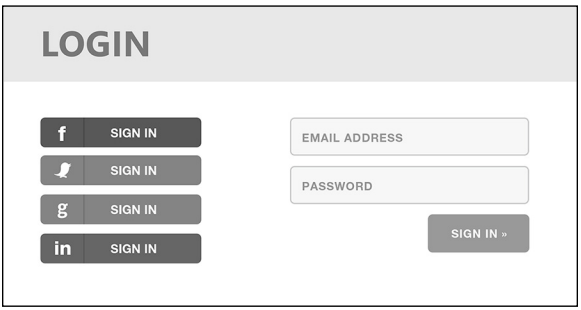

FIGURE 2-4: A single sign on offering.

Cybercriminals also use social media communication and chat to send you an image or video where you're tagged. It may even come from another compromised friend's account and appear legitimate to you. When you see such messages delete, archive, or report them and *do not* click on any links, images, or attachments. If the message appears to come from a friend, message or call that person to verify.

Checking Activity Logs

An *activity log* lets you review and manage what you share on social media. Most Internet accounts and credentials record when and where you log in to your accounts, which browser was used, what you posted, photos you get tagged in, new devices, failed login attempts, and much more.

Get into the habit of reviewing your account activity logs. Get alerts about your logging activity through proactive notifications like the one shown in Figure 2-5. Continuously reviewing your activity log allows you to get familiar with your social activity, be more cautious, and limit what you post.

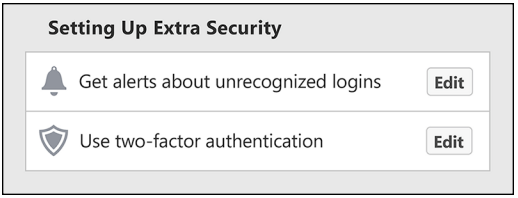

FIGURE 2-5: Setting up extra security for your logins.

Enable login notifications on existing and new devices and browsers. Such notifications of unusual activity are good indicators that your account has been compromised and is now being abused. Also, periodically check your sent emails to check for any suspicious sent email.

Mobile and Bandwidth Usage

Unusually high mobile data and Internet usage can indicate that a device has been compromised and that data is being extracted and stolen. Always review your monthly Internet usage trends (typically available from your Internet service provider or your home router) for both downloads and uploads to monitor your monthly Internet activity. You can typically set limits on usage that will alert you to suspicious levels. When these alarms get triggered, immediately review your usage levels.

Beware of Public Wi-Fi

Data roaming options from telecommunication companies are typically expensive to use in making connections while you're on the road. So when using public Wi-Fi during travels, always make sure to use it with caution and keep the following tips in mind:

- **Always assume someone is monitoring your data whenever you use a public Wi-Fi connection.** Therefore, don't access your sensitive data, such as financial information, don't change your passwords, and beware of entering your credentials. If you have a mobile device with a personal hotspot function, use this over public Wi-Fi.

- **Remove the connections after you've finished joining a Wi-Fi network.** If you don't, you risk what's known as a Wi-Fi Man in The Middle (MITM) attack, which is a Wi-Fi hotspot that uses common Wi-Fi names such as home, airport, café, or free Wi-Fi. When your device sees a known network, it will automatically connect. Make sure to know what networks you are connecting to.


TIP

- **Disable the "automatically join known networks," feature on your portable devices.** That way, when connecting to Wi-Fi, you'll need to review the correct network name and see whether it's secure and protected. ***Note:*** On some devices this feature may be named slightly different, so check your user manual.

IN THIS CHAPTER

- Discovering you've been compromised
- Ransomware, infected devices, third-party alerts
- Notifying boss, colleagues, and friends

Chapter 3
Responding in the Wake of a Cyberattack

With cyber threats, it's only a matter of *when* and not *if* you're going to be impacted. Some attacks are within your control, and some aren't, so you need to be prepared on what to do *when* you do become a victim. Understanding the method of threats you face (covered in Chapter 2) can hopefully help you identify any hack or compromise before it becomes a major incident.

This chapter describes the important steps you need to follow when responding to cyberattacks. They help you reduce the impact of any compromise, prevent it from spreading, and help you get back to normal operations as quickly as possible.

Following Your Company Incident Response Plan

If your company computer or device becomes infected, you should follow your company's incident response plan and report the cyber incident as quickly as possible to the appropriate person. Many companies have corporate IT policies that define acceptable use, password policies, rules and in some cases, incident response

procedures. Every employee should be familiar with these procedures because rapid responses tend to reduce problems or damage from the incident.

These days, some companies have established cyber ambassadors within each department. These people are typically trained and IT knowledgeable and are first-line responders when something suspicious occurs. This approach helps companies quickly review suspicious occurrences or issues and act accordingly — much like emergency responders.


TIP

Given the frequency and evolving nature of cyber threats, every company should establish a well-defined and well-planned incident response process. It can mean the difference between surviving a cyberattack or losing all your data with catastrophic consequences.

Reacting to Ransomware Incidents

If you experience a ransomware message (see Chapter 2 for more info), quickly disconnect and isolate your computer from the network to protect against spreading it to other devices in your network. Remove the network cable, turn off Wi-Fi, and power off the infected device. If the message occurs on a corporate computer, follow your company's incident response plan for the appropriate restore process.

After a ransomware attack has succeeded, you have limited options for how to respond:


WARNING

- Restore your system and files from a backup.
- Start again with a fresh operating system installation and accept that your files are gone forever.
- Pay the ransom amount, but there's no guarantee you'll receive a key to restore your files, so I *do not* recommend this option!
- Hope security researchers or law enforcement can provide alternative ways to get the encryption key to restore your files — this rarely happens.

Obviously, the best action is to prevent this type of attack by not clicking on unknown links.

Fixing Your Personal Devices

If a personal device, such as a laptop, tablet, or cellphone has been infected with malware, seek expert advice from the IT department where you work or from a computer services firm. In many cases, you may need to connect the hard drive of your device to another system that can then scan the file system for a virus or malware. This will also enable you to back up your critical and important files to another removable hard drive so you can conduct a complete reinstallation of the operating system. You should scan your backup files for any sign of the malware and only then restore them.

Assume that any data stored on an infected device has been stolen and is now in the hands of a cybercriminal. You should also assume that any USB devices you may have used with this device are also infected, and they should all be scanned for any sign of the malware.

Be aware that any Internet services you accessed using the infected device have also been compromised, including the passwords for account access to your bank, financial details, email accounts, and social media accounts, including your social logins that connect you with other Internet accounts.

Changing Passwords, Two-Factor Authentication, and More

To minimize the risk that your personal or business accounts will be abused by cybercriminals after an incident, immediately reset the passwords of *all* your critical and sensitive accounts. Start with your bank, email, and social media accounts. When resetting your passwords, make sure to perform this from a private network and not via public Wi-Fi.

At the same time, review your security settings to enable two-factor authentication and review your password manager (if you have one):

- **Two-factor authentication (2FA):** Many password-required accounts also have the ability to enable 2FA, which combines your password with an additional factor required to log on.

This factor is typically a PIN or token that's generated via an SMS text message or mobile phone authenticator app.

- **Password manager:** A password manager helps you in generating strong, long, and complex unique passwords for each account you have. Consider using free password manager software that helps you create these passwords. This security process reduces cyber fatigue and makes it easier to protect your accounts with a password vault. Some password managers allow you to check for the age of passwords, duplicate passwords, and weak passwords.

Notifying Your Boss, Friends, and Colleagues

Notify your family, friends, and your company that you have been the victim of cybercrime and alert them to check their systems and accounts for any signs of suspicious messages or emails coming from your accounts that could be spreading malware. Be aware of the warning signs highlighted in Chapter 2 and review your security settings following the best practices in Chapter 4.

REMEMBER

While some people may be reluctant to share or report that they've been victimized in a cyberattack, it's important to report a cyber incident as soon as possible. A malware infection from a simple email with an attachment could be the first step to a major cyber incident. If unreported, the infection could escalate and impact critical infrastructure or services such as a community power supply, logistics and supply chains, or even hospitals and emergency services that could result in severe damage and possibly loss of life.

IN THIS CHAPTER

- Backing up your important data
- Choosing privacy settings and strong passwords
- Thinking before you click

Chapter 4
Ten Ways to Protect Yourself

The next time you're about to go online — whether at work or home — stop, think, and then connect. Remember that you are both the target of cybercriminals and the strongest line of defense against cyber threats to your employer, your loved ones, friends, and yourself. In this chapter, I give you ten best practices to help you stay safe online.

Back Up Your Important Data

It is always important to have more than one copy of your most important data. Make sure to back it up frequently and keep a safe offline copy to ensure that ransomware or even a technical problem doesn't get in the way. Having a backup is the best way to recover from ransomware (see Chapter 3).

Limit Sensitive Personal Info on Social Media

Whether you're about to create a new social media account or you already have existing ones, make sure that you only enter the

basic information required to get the account activated, and don't provide excessive information that could put you at risk. For more information, see Chapter 2.


TIP

For each account you create, check the minimum required information and think twice about entering data that's classified as Personal Identifiable Information (PII).

Enable Privacy and Security Settings

Many social networks are open to the public by default, privacy is typically basic or turned off, and security is optional. Make sure to review what privacy and security options are available for each account and enable them. Make sure the security is sufficient for the type of data or services you plan to use for your account. Use two-factor authentication (2FA, see Chapter 3 for more info).

Use a Password Manager

If you have many accounts and passwords, opting to use a password manager makes securing and managing your accounts easier. A password manager helps track the age of each password, lets you know what additional security controls have been applied, and helps generate complex passwords for all your accounts so you won't have to type or remember them. You only need to remember *one* strong password, which reduces your cyber fatigue and makes your life easier — and more secure.


REMEMBER

A password manager will help you, but do remember that there are still a few best practices when creating account passwords. You can use *passphrases,* which are a combination of words that you know and a few special characters (for example, ?%&@!). A long, strong passphrase combined with 2FA is tough to crack. Make sure to change passphrases at least every nine months to one year.

Limit Social Logins

Many online services have a social login, also known as Single Sign On. This means that you can sign up for new accounts by using your Google+, Facebook, and so on. This offering solves the

issue of remembering multiple passwords, but it poses a greater security that many people don't realize.

When using Single Sign On, most apps request read/write access or access to your basic information that most people are okay with, but some apps request *full* access, which means access to almost everything including emails, calendar, location information, friends, family, and so on.


TIP

When possible, use unique accounts rather than social logins because if those accounts get compromised or stolen, it means that cybercriminals can cascade to all your accounts just by using the one stolen social login. For more info, see Chapter 2.

Know Your Digital Footprint

If you've never searched for yourself in any search engine, it's time you discovered what your digital footprint looks like. A *digital footprint* is the data that exists in cyberspace as a result of actions and communications that you or others perform online.


TIP

Search yourself online. This action quickly identifies potential fraudulent accounts and then you can take action by automating digital identity alerts to alert you to your personal information found online.

Beware of Public Wi-Fi

When security is important, use your cellular network instead of public Wi-Fi. If you must use public Wi-Fi, ask the vendor for the correct name of the Wi-Fi access point and whether it's secure. Hackers will use Wi-Fi access points with common names like "Airport" or "Cafe" so your device will auto connect without your knowledge.


TIP

Other tips include the following:

- Don't select to remember the Wi-Fi network.
- Use the latest Web browsers because they have improved security for fake websites.
- Use a VPN (virtual private network) service.

Always assume someone is monitoring your data over public Wi-Fi. For more tips, see Chapter 2.

Limit Followers and Access to Social Media

When using social media, be aware of the risks of liking, following pages, or allowing different applications to access your profile because when access is provided, many people don't have good cyber hygiene on cleaning them up when no longer required. Information is shared and unless your followers get revoked, they'll continue to have access to your profile data.

Run Antivirus Scans and Install Software Updates

You can discover if you're a victim of a cyberattack by installing or updating your antivirus software, running a full scan, patching your system with the latest security updates, or changing your password and security. This is why your IT security team at work constantly tells you to change passwords, let antivirus scans complete, or reboot your systems periodically. These processes and techniques help prevent and detect security incidents and apply to your own personal devices (including smart TV or home security cameras) and any Internet user accounts as well.

Think before You Click

We are a society of clickers; we like to click on pictures, addresses, hyperlinks, and more. Always be cautious of receiving any message with a hyperlink, and ask yourself whether it was expected. Do you know the person who's sending it? Ask people whether they actually sent you something before clicking on potential malware.

Improve your cybersecurity now!

CYBERSECURITY DEFENDER TOOLBOX FREE from Thycotic

Download now: thycotic.com/free-tools

FREE

PASSWORD TOOLS FOR EVERY EMPLOYEE

Password Strength Checker	Lets you instantly check a password for its strength in protecting your user account.
Strong Password Generator	Enables you to instantly generate a super strong password that cannot easily be hacked.

FREE

LEARNING TOOLS FOR IT PROFESSIONALS

Privileged Password Security online training course	Makes sure you and your staff are up to speed on the importance of privileged account security and best practices to protect passwords.
Security Policy Template for Privileged Passwords	Saves hours of time and effort with easy-to-customize templates that help you improve security and meet compliance mandates.

FREE

SOFTWARE TOOLS FOR IT PROFESSIONALS

Weak Password Finder for Windows	Gives you an immediate and easy way to identify where the weak passwords are located across your organization.
Privileged Account Discovery for Windows and UNIX	Enables you to find privileged accounts across your enterprise, including many that are unknown and unmanaged.
Windows Endpoint Application Discovery	Saves you hours of effort by discovering vulnerable applications and their associated risks in minutes.

FREE

BENCHMARKING TOOLS FOR IT & RISK PROFESSIONALS

Password Vulnerability Benchmark	Lets you see how your password protection efforts compare with those of your peers.
Security Measurement Index	Online survey shows you how your IT security effectiveness compares with best practices and those of your colleagues.

thycotic

Defend against cyberattacks

Cybersecurity For Dummies, Thycotic Special Edition, helps you understand and recognize the most common cybersecurity threats in your personal and work lives. You discover how cybercriminals target their victims and what you can do to reduce your risk, improve your cyber hygiene, and make it more difficult for attackers to steal your information, your identity, and your money. You are the strongest line of defense against cyber threats for your employer, your loved ones, friends, and yourself.

Inside...

- Identify different email scams
- The risks in social media
- Discovering you've been compromised
- Limiting personal info
- Privacy settings and strong passwords
- Being cautious with public Wi-Fi

Joseph Carson has more than 25 years of experience in enterprise security. He is a CISSP and an active member of the cybercommunity, speaking at conferences globally. He's a cybersecurity advisor to several governments, as well as critical infrastructure, financial, and maritime industries.

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

Also available as an e-book

ISBN: 978-1-119-46735-9
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.