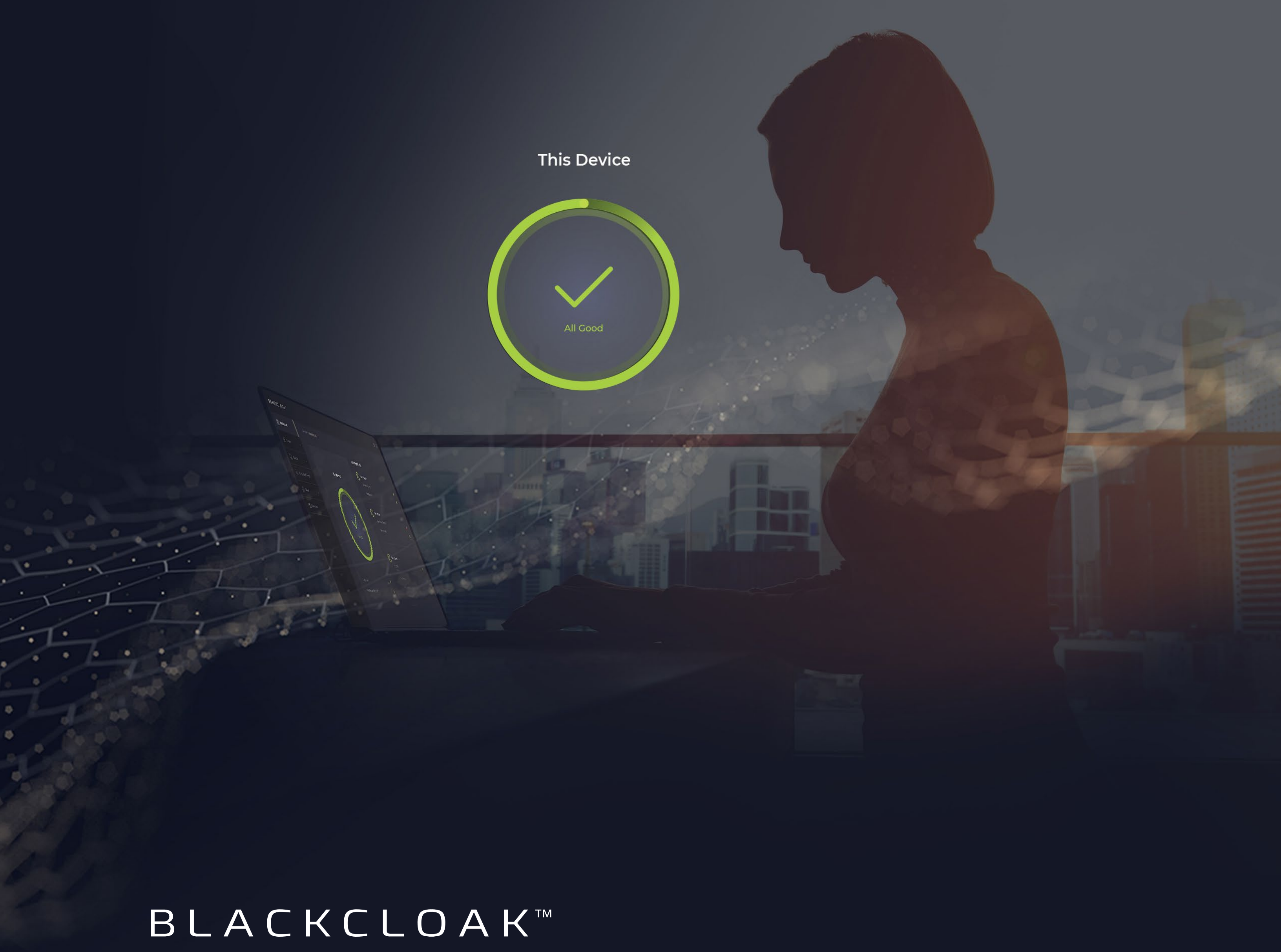


BLACKCLOAK™

The Essential Guide to Cybersecurity & Privacy

FOR HIGH-PROFILE INDIVIDUALS & FAMILIES TO PROTECT THEIR FINANCES & REPUTATION

Contents

Introduction

In today's advanced technological age when a multitude of everyday activities often relies on connecting to the Internet or using a smart device, the importance of cybersecurity grows ever more prevalent.

This is even more true for high net worth individuals (HNWIs), who are purposely targeted on an ever-increasing scale. In fact, HNWIs and family offices are specifically targeted by cyber criminals because about 40% do not have proper cybersecurity protocols in place.[1]

Protecting your data, your assets, and your family is a joint effort.
You can certainly purchase equipment or applications that can add levels of security to your home network, but you'll also need to be aware of other vulnerabilities hackers seek to exploit. Aside from the dangers of malware, ransomware, and poorly protected smart devices, hackers utilize phishing attempts and spoofed websites, among other forms of Internet trickery, to easily get past your defenses.

About 40% [of HNWIs] do not have proper cybersecurity protocols in place.[1]

By availing yourself of the knowledge contained in this eBook, you'll be better informed and equipped to safeguard what you hold most valuable and keep cyber criminals at bay.

Chapter 1

Protecting Your Privacy is Paramount

Privacy.

It's a word that holds particular significance in a multitude of aspects of our daily lives. There are many actions we do every day to ensure our privacy. From pulling down the window shades at night to installing a fence around our property, from shredding documents containing sensitive information to covering up the keypad when we punch in our PIN code while using a debit card, these and many more actions are performed primarily for one specific purpose: to ensure the safety, security, and privacy of our family, our home, our finances, and our identity.

And while you may sometimes scoff at someone's efforts to ensure their privacy, thinking them perhaps a bit too extreme or ridiculous in their actions, there are others who are, in fact, counting on you to feel that way. Because, for every action that you choose NOT to take to ensure your privacy, you leave yourself vulnerable in a manner that hackers, scammers, cyber criminals, identity thieves, and other unscrupulous individuals can take advantage of.

> “
>
> **For every action that you choose NOT to take to ensure your privacy, you leave yourself vulnerable in a manner that hackers, scammers, cyber criminals, identity thieves, and other unscrupulous individuals can take advantage of.**

Why Privacy Should Come First — How Lack of Privacy Leaves You Vulnerable

Today's world is full of risks lurking around every corner, in both the physical and the digital landscape. This statement isn't necessarily meant to scare you or to encourage you to think that you should avoid ever going outside or using an Internet-enabled device. Rather, it is simply meant to encourage you to be careful, utilize common sense, and take the proper precautions to ensure your privacy and eliminate critical vulnerabilities in your home and in your digital footprint.

What does privacy mean to you and/or your family?

How seriously do you take your privacy?

What do you consider to be the largest threat to your privacy?

A survey conducted in 2019 asked Americans what privacy meant to them.[2] The majority focused on the idea of shielding their personal information from organizations that would use it for learning more about them, such as government agencies, big companies, or social media platforms.

To a lesser extent, the concern was for those that would utilize personal information for illegal activities, such as identity theft. This is problematic. It means the majority of Americans don't realize that privacy has a direct impact on their financial well-being.

Fraud Fact:

The Federal Trade Commission (FTC) estimates that as many as 9 million Americans have their identities stolen each year.[3]

Fraud Fact:

Cyber criminals have caused over $3.5 billion in losses last year.[4]

Privacy for Physical Security

Obviously, keeping your data private and secure is critical, but you certainly shouldn't neglect your physical security either. Your reputation and finances aren't the only things that are in danger when you don't practice proper cybersecurity.

Consider your doorbell and security cameras, as well as the cameras on your computers and mobile devices. Savvy hackers can re-use your compromised credentials (username/password) or use malware to breach the cameras to see if anyone is at home.

DID YOU KNOW? *Camfecting* is the process of attempting to hack into a person's webcam and activate it without the webcam owner's permission. (You might have heard it referred to as webcam *hacking*.)

Likewise, personal information sold on data broker websites can be used to reveal your home address.

And let's not forget about social media — are your social media accounts private or public? Posting those amazing vacation photos to the world also showcases a home that is currently empty. Family photos in the home may give criminals a good idea of the layout of the home, what valuables could be inside, and even what type of security system you may have.

Top 5 Reasons to Keep Personal Information Private

1. Peace of Mind and Family Protection
2. Prevent Identity Theft & Keep Your Finances Safe
3. Protect Your Reputation & Your Company's Brand
4. Maintain Your Employability
5. Prevent Robberies and Burglaries

Practice Safe Social Media:

- Enable dual-factor authentication (also called two-factor authentication or 2FA) on your social media accounts.
- Don't use the same password as you always use for your social media accounts.
- Change your privacy setting to 'friends' or 'friends of friends' rather than being fully public.
- Avoid posting details about your schedule, such as when you are at work or when you're going on vacation.
- Don't accept friend requests from people you don't know.
- Turn off search engine indexing — this prevents search engines from linking to posts in your timeline.
- Initiate 'tag request' approval so that you cannot be automatically tagged in other people's posts without your approval.
- Avoid linking posts from different social media platforms, since other platforms may be more public.

> Regardless of the tactic used or the message received, the ultimate goal is usually to gain the means to access your private accounts.

Privacy for Cybersecurity

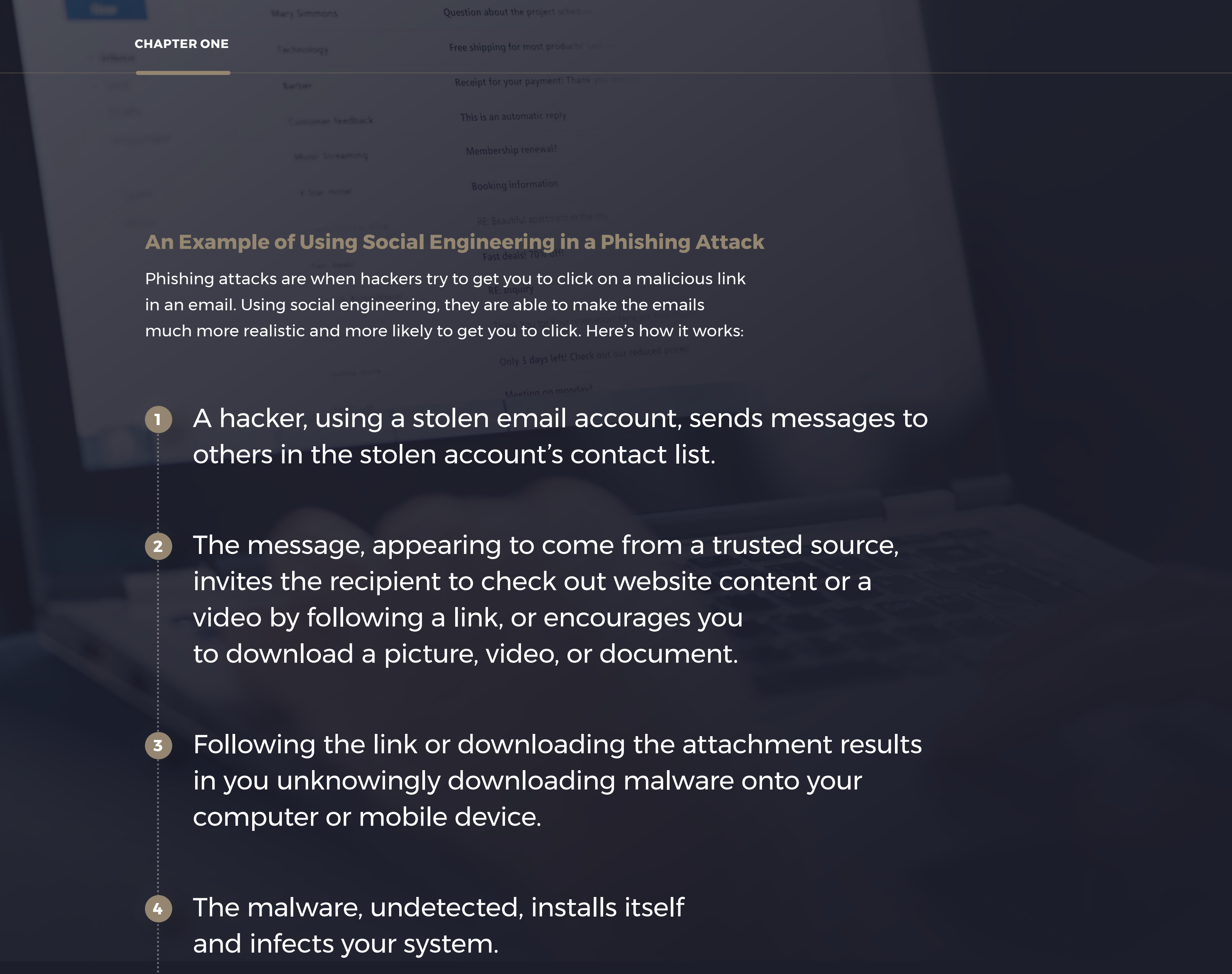
Being aware of your surroundings, whom you talk to, and what information you provide to others are also important things when it comes to cybersecurity risks. Have you heard of social engineering? Not many people have, but criminals are using social engineering tactics every day to trick you into giving up personal information.

Social Engineering Attack: What is it?

A social engineering attack occurs when a criminal targets an individual and attempts to exploit them via trickery, taking advantage of both their curiosity and their trustworthiness. Such tactics are typically employed by criminals when they feel it will be easier to obtain the information they seek that way, rather than by attempting to hack into your network.

Social engineering tactics can vary, but typically entail a phone call or an email message that imparts a sense of urgency, such as a friend in need of assistance. Other variations include notifying you that an account will be closed or is locked, asking for donations to a charitable cause or fundraiser, advertising a free service, or presenting you with an issue with one of your accounts that requires you to sign in via the link provided.

Regardless of the tactic used or the message received, the ultimate goal is usually to gain the means to access your private accounts.



An Example of Using Social Engineering in a Phishing Attack

Phishing attacks are when hackers try to get you to click on a malicious link in an email. Using social engineering, they are able to make the emails much more realistic and more likely to get you to click. Here's how it works:

1. A hacker, using a stolen email account, sends messages to others in the stolen account's contact list.
2. The message, appearing to come from a trusted source, invites the recipient to check out website content or a video by following a link, or encourages you to download a picture, video, or document.
3. Following the link or downloading the attachment results in you unknowingly downloading malware onto your computer or mobile device.
4. The malware, undetected, installs itself and infects your system.
5. The hacker then has the ability to record your keystrokes, and will be able to acquire usernames and passwords to your private accounts. The malware might also have the ability to copy other data stored on your computer or mobile device, take over the device's camera, or even take control of your entire computer system.

DID YOU KNOW? Phishing emails are the most common type of social engineering. Less common tactics include baiting, vishing, tailgating, pretexting, and smishing. Nearly 91% of all cyberattacks start with a phishing email.[5]

6 Types of Social Engineering Attacks

Phishing

Emails that trick a target into clicking on a link, opening a document, or logging into some website with your credentials.

Baiting

An offer that entices a target and tricks them into downloading malware or entering personal information.

Vishing

A social engineering attack carried out via a phone call.

Tailgating

Occurs when a person who is not authorized to enter a particular area follows in one who is authorized.

Pretexting

Occurs when a scenario is created that causes a target to lower their guard and reveal sensitive data.

SMS-based

An SMS based phishing attempt (i.e. via text messaging on your mobile device).

Cybersecurity Tip: Recognizing and Avoiding Phishing Emails

If you receive an email that appears to come from a trusted individual or organization, follow these steps to ensure it is not a phishing attempt.

1 Read the email carefully

Phishing emails typically contain a message that conveys a sense of urgency, such as a request for help from a friend or your bank informing you that a security issue was detected. Scammers want you to act before you think. Take the time to read the email thoroughly and examine the message. Many phishing emails can be easily detected when you take the time to give them a second glance.

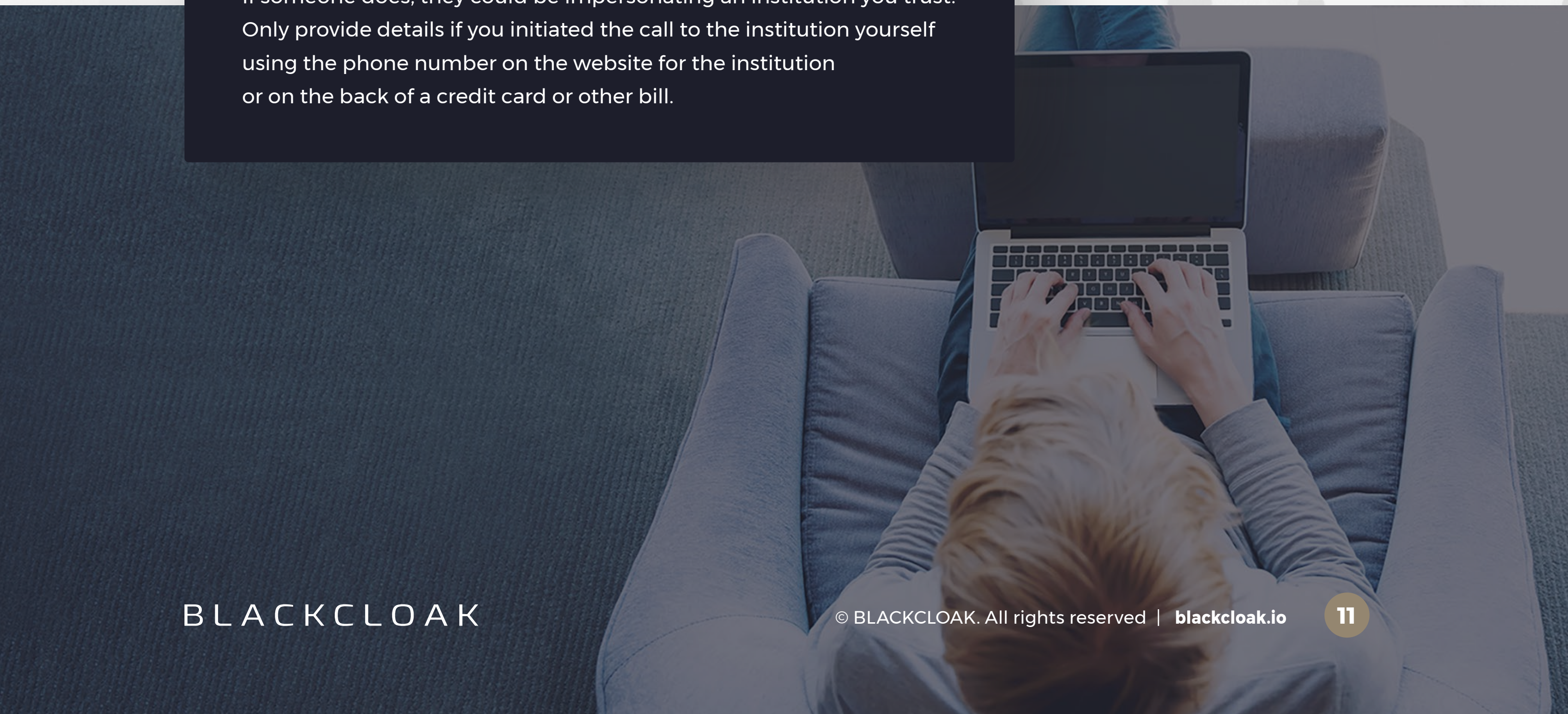
- Does the message contain numerous spelling and grammatical errors?
- Does the message come from an organization that you don't even have an account with?
- Does the message ask you to click on a link, call a number, or input your information?

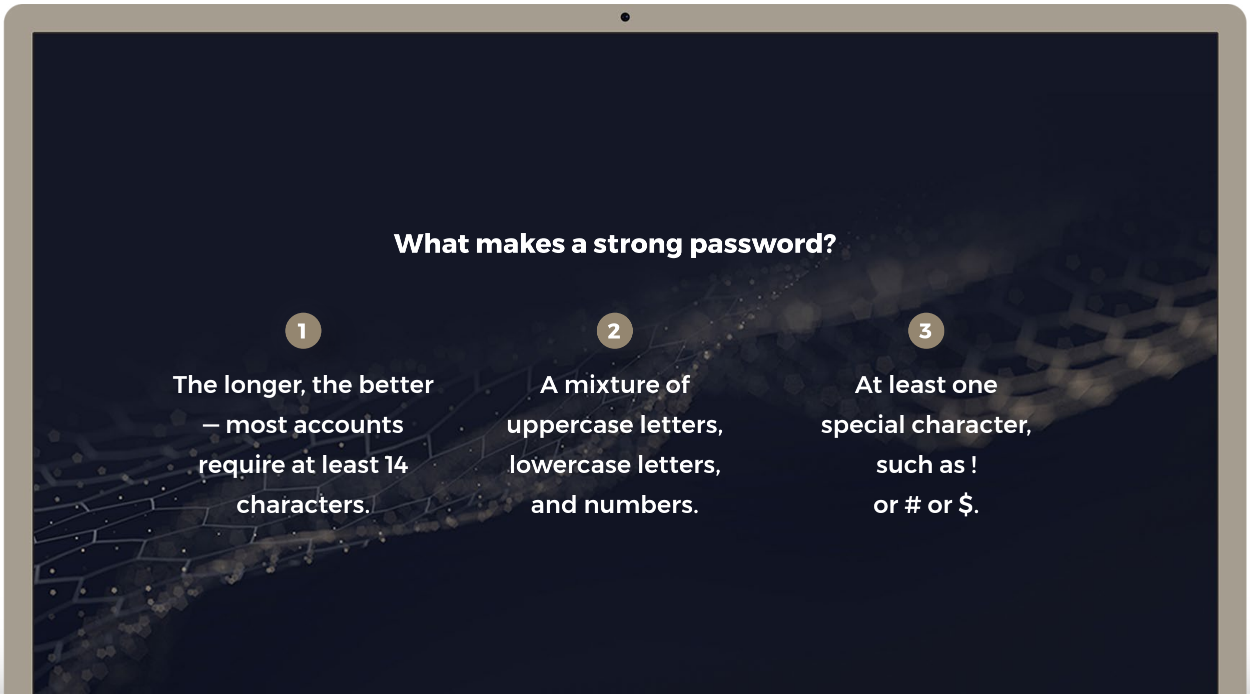
2 Never click on the link in an email

The links in phishing emails typically lead to cleverly designed, fake websites that mirror the actual website of the organization. Sometimes clicking on the link also initiates a download of malware without your knowledge.

Hovering your cursor over the link can usually clue you in to whether or not the link is real or fake. But to be certain, simply type the real URL into the address bar yourself. Then you can be certain you are going to the actual site instead of a fake one.

SECURITY TIP: Never give out personal information over the phone to anyone that calls. Major organizations and financial institutions will never ask for private account details over the phone.
If someone does, they could be impersonating an institution you trust. Only provide details if you initiated the call to the institution yourself using the phone number on the website for the institution
or on the back of a credit card or other bill.





What makes a strong password?

1. The longer, the better — most accounts require at least 14 characters.
2. A mixture of uppercase letters, lowercase letters, and numbers.
3. At least one special character, such as ! or # or $.

Passwords

Obviously, you want to keep these passwords private and secure, because if someone were to discover your password and log in to one of your accounts, they will have gained the potential to not only discover more sensitive data about you and your family, but also wreak havoc with your finances or your reputation.

SECURITY TIP: Use a password manager tool to generate strong passwords and keep track of them, so you don't need to try to remember them all. We recommend LastPass and 1Password

Social engineering (particularly phishing emails) are meant to try to get your passwords to various accounts, but even if you don't give up the password, revealing a few key pieces of information can be enough for a savvy hacker or cyber criminals to successfully guess your password.

For example, your mother's maiden name, the place where you were born, your first pet's name, and other similar information are often the answers to security questions asked by accounts you are trying to log into when you forget your password. With enough information garnered by social engineering, a hacker could use it to acquire your password. Maybe your pet's name is your password! (If it is, change it right away!)

To ensure top security that makes it increasingly difficult for a cyber criminal to discover your passwords, use a different, strong password for each account.

Identity Theft

Trust us, the last thing you ever want to deal with is trying to restore your finances and a sense of normalcy after being victimized by an identity thief. And that's exactly why eliminating vulnerabilities and protecting your privacy is so important. The more a hacker, identity thief, or cyber criminal knows about you, the easier you make it for them to successfully steal your identity.

Fraud Fact:

Children are increasingly the victims of identity theft — 51% more than adults.[6] Identity thieves target children because their social security numbers are cleaner, lacking a credit history, and thus can be more easily used to establish a fake identity and open new accounts. This is called synthetic identity theft.

Top Ten Things Everyone Should Do for Better Security

1. Never give your SSN to anyone unless a necessary requirement (such as for taxes, banks, employers, etc.)
2. Don't carry your SSN card and other sensitive documents with you unless you need to (passports, birth certificates, etc.)
3. Invest in travel-related physical security (RFID protector, anti-theft pouches, etc.)
4. Avoid using public Wi-Fi services to sign into private accounts
5. Avoid giving up personal details to people you don't know well
6. Make your phone lock as secure as possible
7. Increase security for your personal Wi-Fi router
8. Never send sensitive information over email unless it is encrypted
9. Turn off location settings on photos you take and don't post photos showing you away from home until you are back at home
10. Use a shredder for all documents with personal or financial information

Chapter 2

Protecting Your Home is Needed More Than You May Know

Hackers and cyber criminals are taking full advantage of today's ever-advancing technology and our reliance on it. And, while large data breaches against major corporations are often reported in the media, you don't hear about the hundreds of thousands of cyber attacks committed against people in their own homes. But being aware of the vulnerabilities in your home network, as well as the devices used in or around the home, can significantly reduce the risk of a successful breach.

DID YOU KNOW? Experts estimate that a hacker infiltrates an account or network every 39 seconds.[7] And, 3 out of 4 Americans have had to change passwords for at least one private account due to a security breach.[8]

Identifying the Vulnerabilities

We've all heard the stories about our smartphones, smart devices, and apps listening in to our conversations and transmitting data back to some faceless entity. These systems are designed to provide consumer information to corporations for better demographic targeted marketing purposes. This behavior, although not exactly welcome, is not the type of vulnerability you necessarily need to be worried about.

The threats to your privacy that warrant greater attention and concern are those committed by cyber criminals engaging in attacks against your IoT devices, routers, and cameras. Homes that contain a greater number of Internet-connected devices face a greater risk, especially when the proper steps aren't taken to eliminate vulnerabilities and protect your digital privacy.

Vulnerabilities in Your Home Network

A home network is particularly vulnerable to cyber attacks simply because there are so many tactics a hacker might employ to gain unauthorized access. Whether a cyber criminal is seeking to exploit human carelessness through tricky social engineering endeavors, or they are attempting to exploit security gaps in the hardware, your network's defenses can be particularly tricky to control without multiple levels of comprehensive cybersecurity protection.

Essentially, your home network is vulnerable on three fronts: the hardware, the software, and human error.

Hardware — Routers and other hardware devices need to be updated with the latest firmware and system applications in order to ensure any security patches are installed. Hackers are constantly working to discover new flaws in a device's firmware; regular updates typically patch these security gaps.

Malware that is unknowingly installed on a device can also enable a cyber criminal to take over your home network. Spyware can allow a hacker to see all your keystrokes, providing them with usernames and passwords to your private accounts.

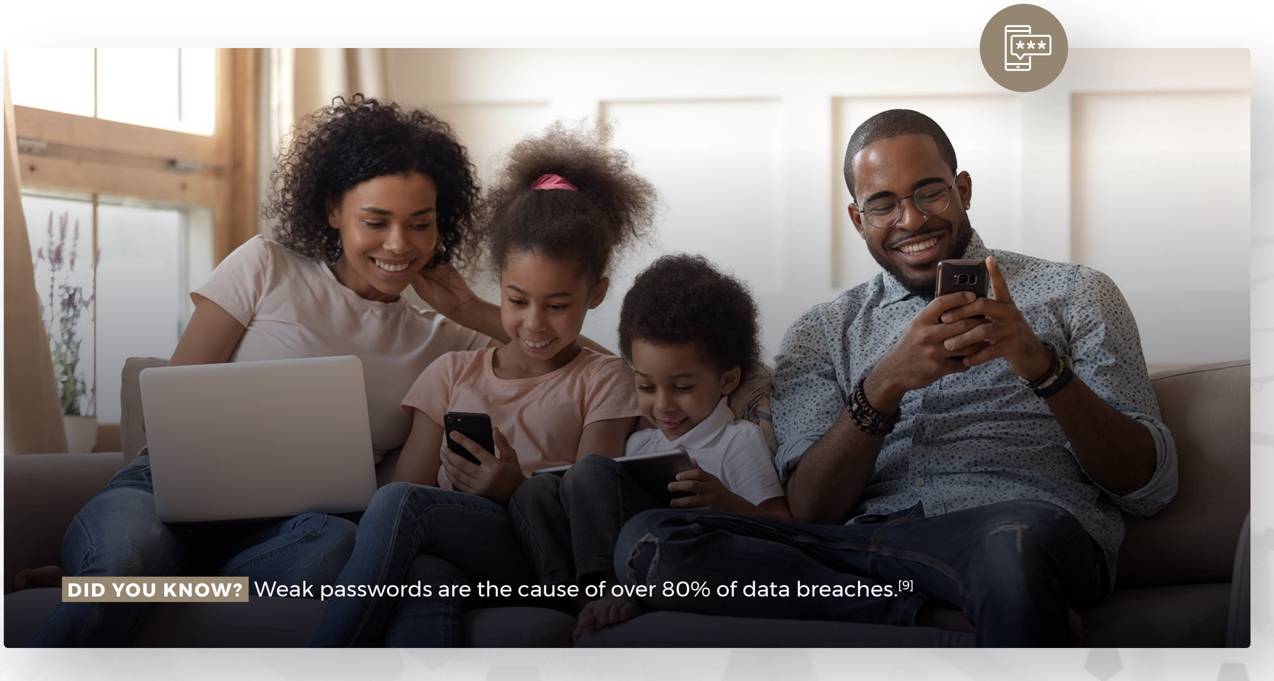
Misconfigured or unpatched firewalls sometimes aren't enough to protect your home network from a criminal's attempts to infiltrate it, either. And a poorly secured Wi-Fi network allows criminals to easily get past your firewall.

Software — Like your hardware, software applications also often receive regular updates, and these can be just as important as the updates for your router or operating system. Hackers can discover and exploit flaws in various applications to gain access to your home network.

Outdated software, software applications that aren't being used much anymore, and third-party plug-ins can also increase your home network's vulnerability.

Human Error — Even when you have everything on your home network properly updated and secure, a simple error in judgment can open the digital doorway for hackers and cyber criminals. Some of the ways criminals gain access to your home network via human error include:

- ✓ Using weak passwords
- ✓ Using the same password for multiple accounts
- ✓ Not recognizing phishing emails
- ✓ Downloading files and documents that contain malware
- ✓ Clicking on links that lead to cleverly designed, fake websites



DID YOU KNOW? Weak passwords are the cause of over 80% of data breaches.[9]

IoT Vulnerabilities

The Internet of Things (IoT) consists of all manner of smart and Wi-Fi-enabled devices we use in the home. While many of these devices offer a great amount of functionality and convenience, they are also often designed with poor security. Many of them are also incapable of being updated with new firmware, leaving them prime targets for cyber criminals.

DID YOU KNOW? The average home has eleven smart devices.[10]

Vulnerabilities in Camera Systems

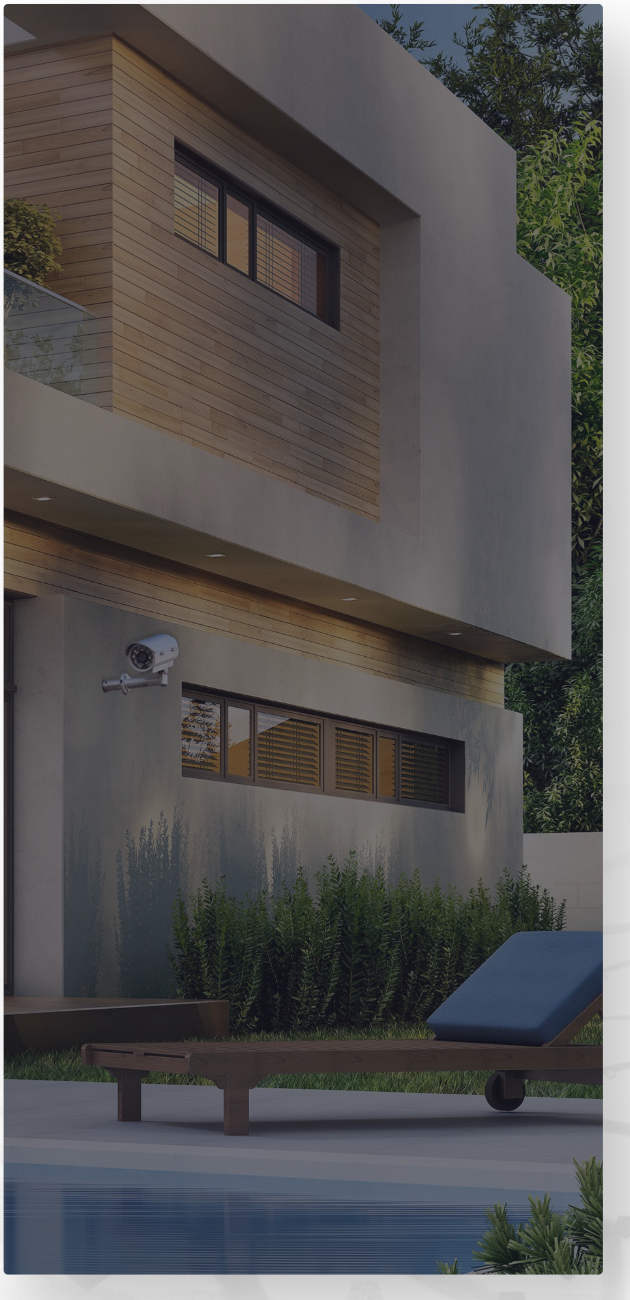
Today's home typically has two camera systems — those designed for security, such as security system cameras or doorbell cameras, and those that are attached to devices such as smartphones or desktop and laptop computers.

You wouldn't think that your security system cameras could be hacked, but, unfortunately, you'd be wrong. Many of today's home camera systems are connected to your home network, which makes them vulnerable if not properly secured against cyber attacks. Criminals can use the hacked camera system as a backdoor to your home network, or they can use your own cameras to spy on you.

This is often the issue with cameras on mobile devices and computers. But in addition to using those cameras to spy on the owners, hackers could also gain access to stored photos and videos on the device, and even take their own photos and videos via a connected application. In some cases, if the camera is on a smartphone, the criminal could even listen to and record private phone conversations.

Vulnerabilities in Home Automation Systems

Home automation systems offer a magnitude of convenience, but, you guessed it — security vulnerabilities as well. As part of the IoT, home automation systems are also connected to your home network, and each device that is a part of the system is a potential risk factor for unauthorized access. Many of the devices are simply built without proper security measures, making them fairly easy to breach.



Best Practices for Securing Home Networks

Now that you know the security risks, you can take steps to improve the security of your home network and connected devices. The majority of these steps consist of simple, common-sense practices that will significantly reduce the risk of a successful cyber attack or data breach.

Use Two-Factor Authentication (2FA)

This adds an extra level of security to each account that is the primary deterrent of hacking and phishing attempts. This is usually an extra code that is texted to your phone, but can be other, harder to hack, methods as well.

Always Update

Always ensure that any operating systems, applications, and firmware is up to date with the latest versions and security patches. Many updates can be set to be automatically enabled.

Enable Guest Wireless

Set up a separate guest Wi-fi connection for visitors, preventing them from gaining full access to your private network.

Invest in Security Software or Cybersecurity Services

Multiple layers of security that improve your firewall protection and monitor your network will protect against malware, viruses, phishing attempts, malicious websites, and more.

Use Strong, Separate Passwords for Each Account

Passwords are especially important. Use a password manager to generate and keep track of unhackable passwords.

Use Wi-Fi-Protected Access (WPA2)

Doing so will better protect your wireless communications.

Back Up Your Data

Keep your data backed up in the Cloud or on portable drives. In the event of a data loss or ransomware attack, you'll be able to retrieve your important data.

SECURITY TIP: Beware of downloads in emails, even if they come from a trusted source. Hackers can take over email accounts and send malicious apps and spyware disguised as other files to everyone in the individual's contact list.

Securing Your IoT Devices

Sometimes there just isn't much you can do to secure some IoT devices, so the first thing you should do in order to ensure better security is to invest in a more secure router. Once you do, be sure to change the name, so that others who can see your network won't be easily able to identify the make and model router. Then:

1. **Use 2FA if available to log into your devices.**
2. **Use a strong encryption method for your Wi-Fi, such as WPA2.**
3. **Keep your network private; don't give your password to visitors. Instead, set up a guest network that visitors can access but that isn't connected to all your IoT devices.**
4. **Change the default usernames and passwords for your router and all IoT devices.**
5. **Use a strong, unique password for each device.**
6. **Check the privacy settings for any device; you can sometimes change the default settings to enable more security.**
7. **Keep software up-to-date and enable automatic updates for any devices.**
8. **Don't attempt to manage your IoT devices while using public Wi-Fi.**

DID YOU KNOW? Cyber criminals most often access IoT devices simply by trying the default passwords for the devices that were never changed.

Securing Camera and Home Automation Systems

With many home security cameras and home automation systems, your only option for improving the security of the devices is to be sure the firmware is updated and the default password is changed. And, as with other devices connected to your home network, keep your router secure.

Adjusting some of the router settings can make a big difference in eliminating potential vulnerabilities. For example, turning off the Universal Plug and Play (UPnP), which is often a security issue, can reduce the risk of hackers accessing your home network.

If your router comes with WPA3 encryption, choose that instead of WPA2. It provides stronger security but isn't available on all models yet.

It's also a good idea to occasionally check the IP logs of your camera. This will provide you with a list of the IP addresses that have accessed the camera feed. If you see any that aren't your own, then someone might have attempted an unauthorized breach. Change your password and call your security provider.

When it comes to the cameras on your computers or mobile devices, many of the same rules apply. Keep system software up-to-date, use a firewall to provide additional security for your desktop and laptops, and keep your Wi-Fi network secure.

You might also consider a VPN. A virtual private network adds an extra layer of privacy and security to all your Internet-related actions, deterring hackers.

HOW TO TELL IF YOUR WEBCAM IS HACKED

A sure sign that your webcam might be hacked is if you notice the indicator light on, but you did not initiate the camera to run yourself, it is likely under the control of a hacker. However, savvy hackers can also disable the indicator light.

To be sure, review the logs of access and use to the web portal or software used to control the webcam.

Chapter 3

Protecting Your Devices

Hackers have numerous methods for discovering and targeting devices. And every day, savvy cyber criminals are attempting to develop new methods for hacking mobile devices and computers.

Where and How Hackers Target Devices

To find a device to hack, cyber criminals typically use network scanning tools. They might also make use of a specialized search engine called Shodan, which discovers and catalogs devices that are connected to the Internet. Once a hacker finds a router or similar device that might provide access to a home network, they will initiate the process to attack the device.

To start, they might simply try accessing your devices using common default passwords, since many individuals fail to change them. Additionally, if the hackers manage to discover a password for one device, they will likely attempt to infiltrate other devices with the same password, since homeowners have a tendency to use the same password on multiple devices and online accounts.

No matter how hard manufacturers try to build secure products, all hardware and software have some vulnerability. Often these vulnerabilities are discovered after product release, and hackers use those known vulnerabilities to get into your device. Manufacturers release patches for these vulnerabilities, but you have to keep your software or system up-to-date to get them. Zero-day vulnerabilities are newly discovered and do not have patches yet.

Once the Hacker Gets In

When a hacker manages to infiltrate a home network or even a single Internet account, there is the potential for a great amount of illegal activity to be committed. From stealing or erasing data to controlling devices, to identity theft and more, a breached system or account can result in continuous headaches and financial difficulty for you and your family.

What Can a Hacker Do to Your Computer?

- Take over your computer or mobile device
- Steal your personal data
- Encrypt all of your data, make it inaccessible to you, and ask for a ransom or they'll publish all the information for the world to see
- Delete data and applications
- Download viruses or malware to your computer or device
- Access your bank accounts or steal credit card numbers
- Steal and sell passwords
- Use your computer to attack other computers

Obviously, protecting your devices and your computer is of the utmost priority. You've already read that using strong, unique passwords for each account and device, and protecting your router is of critical importance. There are additional security measures you can take to ensure optimal levels of protection.

DID YOU KNOW? The average device is the target of an average of five attacks per day.[11]

The Tools You Should Have to Protect Your Devices

Anti-Malware Solutions

Having some method of protecting your device from malware is a must-have. This ranges from anti-virus software to software-based firewalls, but it is essential to protect your data from viruses, trojans, and other forms of malware.

Password Management Applications or Vaults

A strong, unique password for each account, as well as your router, is critically important for ensuring privacy and security. A password manager is an excellent resource for creating strong passwords, and then remembering them.

With a password manager, you only need to remember one password — the one for the password manager itself. Then, with the password manager, you can easily generate unbreakable passwords for each and every online account. And you don't need to worry about having to spend extra time logging into accounts either. The password manager makes logging in even quicker and simpler, while still maintaining optimal privacy.

Some password managers will also store credit card information for you and if you are using an encrypted password manager or vault this is safe to use.

Two-Factor Authentication (2FA)

Two-factor authentication (2FA) is a method of establishing access to an online account or computer system that requires the user to provide two different types of information. Not every online account will offer the option for 2FA, though more and more are adding it every day. To increase security on accounts, you can utilize apps such as Authy or Google's authenticator app when the website or application allows for it. This adds an extra layer of security that deters hackers and cyber criminals.

Mobile Device Tracking Tools

Mobile devices sometimes get lost or stolen, despite our best efforts to prevent it. When that happens, a tracking tool can help you quickly locate the missing device. Some tools even offer a feature that can erase data on the device if you feel it is required.

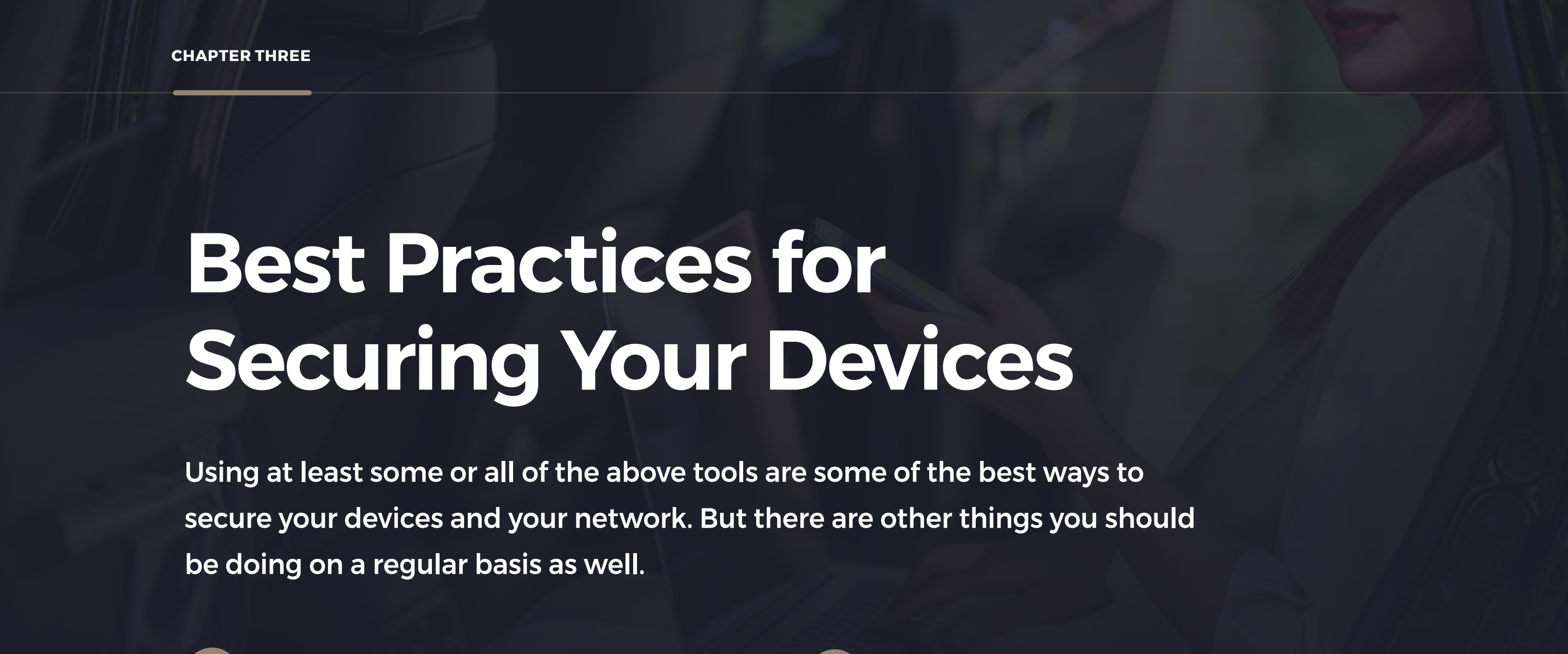
A Virtual Private Network (VPN)

A virtual private network is another must if you often utilize public Wi-Fi. Even if you aren't signing into private accounts when on a public Wi-Fi network (which you shouldn't), a VPN is still beneficial since it encrypts all your data and prevents snooping. If you don't want to use a VPN, then consider using your phone's hotspot instead.

DID YOU KNOW? As many as 81 percent of people use public WI-FI when given the opportunity, exposing themselves to a series of risks.[13]

Security Fact:

More than 24,000 cases of mobile malware are blocked on a daily basis.[12]



Best Practices for Securing Your Devices

Using at least some or all of the above tools are some of the best ways to secure your devices and your network. But there are other things you should be doing on a regular basis as well.

Always Update

Although it can be annoying to get update alerts so often for all your different applications, as well as your system software or firmware, don't ignore them. These updates more often than not fix security flaws in previous versions that hackers sought to take advantage of. When available, adjust settings to allow for automatic updates. And even if auto-update is turned on, periodically check that updates are occurring. Sometimes, not enough available storage on a device can stop an update from happening.

Secure Your Browsers

Make sure your browsers are set to the highest levels of security and regularly patched. A secure browser, in conjunction with a secure VPN, results in a more secure network. Additionally, secure browser settings prevent code from being executed without your authorization or awareness.

Don't Download From Unverified Sources

Nothing, absolutely nothing, should ever be downloaded unless you can be 100% certain it is from a verified, trusted source. If a web page doesn't look exactly right or you can't be certain who sent you an email attachment, don't download anything or even click on a link.

Protecting Your Devices From Other Threats

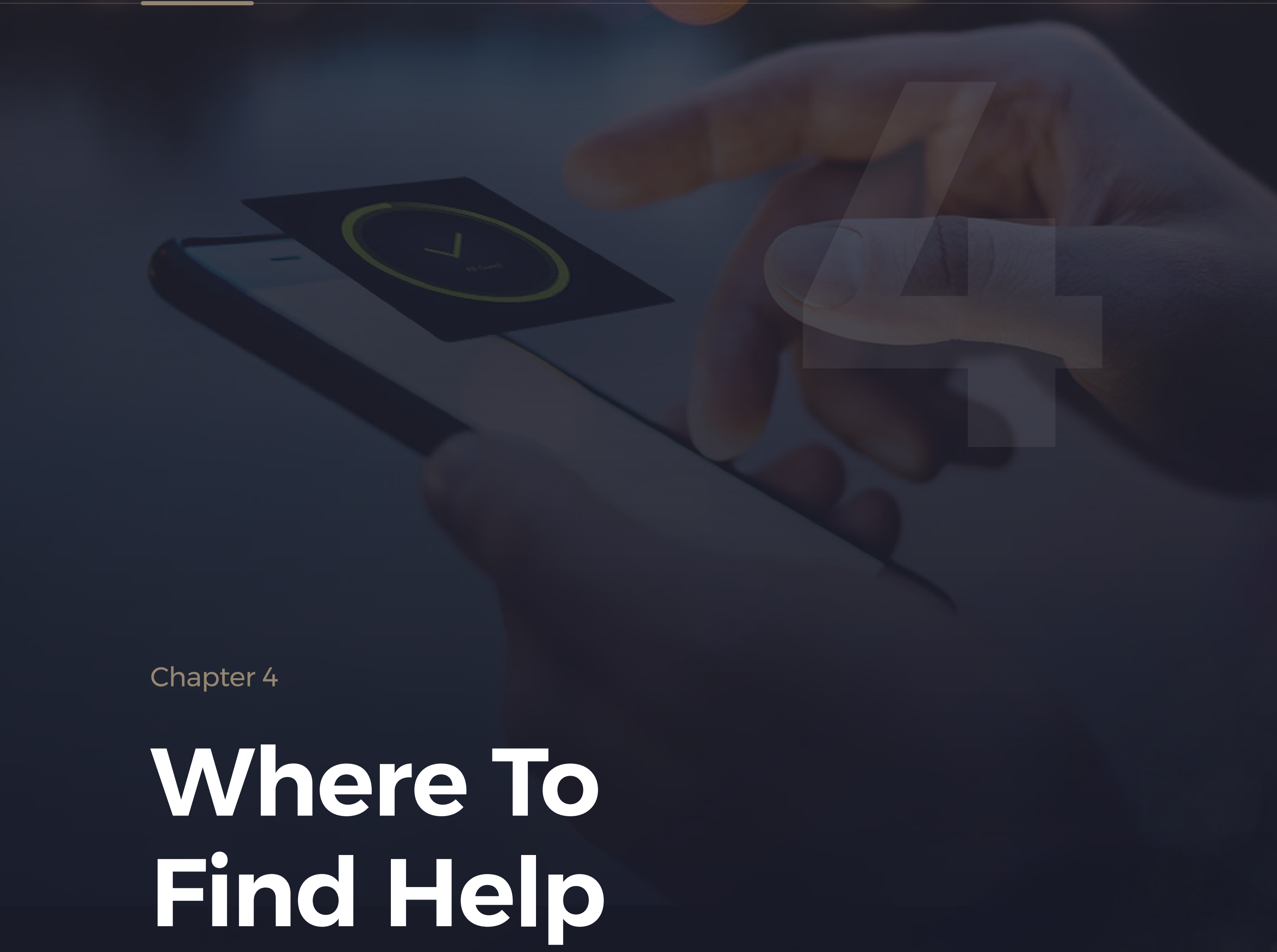
Sometimes a hacker or cyber criminal leaves the dirty work up to you. Instead of trying to access your devices or home network with their own tools or via malicious websites, they simply wait for you to use a USB flash drive or charging port that has been pre-installed with malware.

Did you ever find a USB flash drive just lying around? Many people do, and, of course, are quite curious as to what it may contain. And that is exactly what hackers are relying on. Once the flash drive is inserted into a computer, the malware infiltrates the system, and the hacker now has physical access to the computer.

So, for starters, never use a flash drive if you don't know where it came from. Second, don't use the same flash drive between work and home. This will prevent the risk of cross-contamination.

It is also recommended that you avoid using public USB charging ports. These could contain malware as well. Criminals could also leave portable charging stations plugged into outlets at hotel lobbies, airports, coffee shops, etc., and simply wait for someone to plug their device in to charge.

Avoid these charging ports and only use AC power outlets instead. You can also purchase a device called a "USB Data Blocker," which will prevent data from moving between the port and the device.



Chapter 4

Where To Find Help

While the previous chapters provided a wealth of important and actionable information that can help you minimize the risk of cyber attacks, frankly it can all be overwhelming. Depending on your risk-level (for example, how high-profile a target you are or how much time you spend online), your personal cybersecurity can add up to being a full-time job. There are services that can help provide even more security. There are pros and cons for each, so you'll want to perform your due diligence on each solution so that you can make an informed decision.

Types of Services Providers — Pros and Cons of Each One

Do It Yourself with Consumer-Grade Solutions

There are a multitude of consumer-grade solutions to choose from — from anti-virus software applications to highly secure firewalls and routers. There is no discounting the fact that these play a necessary role in setting up a level of security for your home network. And they can also be fairly inexpensive to purchase, but tend to be difficult to set up and manage.

However, the fact remains that they just don't offer the same high level of security that can be gained via advanced cybersecurity solutions, which are becoming much more of a necessity in today's risky digital landscape, especially for high-profile or high-net-worth individuals who are often targeted by sophisticated criminal organizations.

Consumer-grade solutions also don't cater well to modifications or improvements. They are designed to perform a specific function, and if you want to improve upon those functions, you typically need to purchase newer versions of the software or hardware. And if there aren't frequent updates, these solutions become more vulnerable to cyber criminals every day.

> Depending on your risk-level ... your personal cybersecurity can add up to being a full-time job.

> The ideal solution for high-profile individuals and corporate executives in their personal lives to protect their family, reputation, and finances is a Concierge Cybersecurity & Privacy™ platform.

IT Consultants and Companies

IT consultants can provide you with insight into how best to leverage your technology for optimal benefit. They may also be able to analyze your current network and make recommendations on what you need to do to improve your security. But costs and proficiency levels can vary widely, especially when dealing with IT consultants that charge by the hour.

IT consultants typically don't provide a dedicated, continuous service. Rather, they offer guidance and instruction on what technologies to purchase, and otherwise have limited interaction. There may also be some downtime when they are needed to fix a particular problem with your network, as well as an additional cost.

Managed Security Service Providers

Adequate protection for your home network today requires a great deal more than just anti-virus software and a good firewall. And that's where MSSPs come in. Managed security service providers offer a wide range of services to improve upon current security adaptations as well as enable additional advancements for increasing productivity and efficiency.

As such, they are actually more suited to working with businesses and organizations, rather than individual family networks. While an MSSP might offer security expertise, you could wind up paying extra for a host of services that you don't really need or can't take full advantage of in your home/personal life. Additionally, MSSPs are really meant to supplement an already existing security team, not serve as a personal cybersecurity force.

Concierge Cybersecurity & Privacy Platform

The ideal solution for high-profile individuals and corporate executives in their personal lives to protect their family, reputation, and finances is a Concierge Cybersecurity & PrivacyTM platform. This is a personal subscription software plan with white-glove client support that is dedicated to providing advanced security and privacy services on a 24/7 basis. A security team is always standing by to assist in any problems, and constant network monitoring will detect, prevent, and eliminate threats of malware or other cyberattacks.

For the best in concierge cybersecurity and privacy, choose BlackCloak.

About BlackCloak

BlackCloak offers a holistic solution that combines software and services for both cybersecurity & privacy to help you protect your family, your reputation, and your finances.

The BlackCloak Concierge Cybersecurity & Privacy™ Platform is a holistic solution combining software and services for both cybersecurity & privacy to help you protect your reputation, your finances, and your family.

We remove sensitive personal information from Internet Data Brokers, perform dark web searches for exposed personal credentials, and implement privacy settings to protect against data leakage and identity theft.

We perform penetration testing and regular scans of your home networks to detect compromised networks, weak cybersecurity, BotNets and other security issues, and to prevent decisions children and family make online from resulting in a compromise.

We monitor and secure your personal devices, including cell phones, tablets and computers, using the same enterprise-grade tools used to secure corporate networks and devices.

With BlackCloak as your trusted partner, you'll protect what matters most and have control over managing your cybersecurity and privacy risk — and your personal advisor will always be just a call, tap, or text away.

Sources

[1] *https://www.owensgroup.com/cyber-security-for-high-net-worth-individuals/*

[2] *https://www.pewresearch.org/internet/2019/11/15/how-americans-think-about-privacy-and-the-vulnerability-of-their-personal-data/*

[3] *https://www.crimemuseum.org/crime-library/silent-crimes/identity-theft/*

[4] *https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/*

[5] *https://purplesec.us/resources/cyber-security-statistics/*

[6] *https://www.npr.org/2017/10/18/556237149/to-protect-children-from-identity-theft-parents-must-be-proactive*

[7] *https://www.cybintsolutions.com/cyber-security-facts-stats/*

[8] *https://www.securitymagazine.com/articles/94444-4-of-americans-have-had-to-change-password-due-to-security-breach*

[9] *https://www.infosecurity-magazine.com/blogs/pwned-passwords-business-risk/*

[10] *https://variety.com/2019/digital/news/u-s-households-have-an-average-of-11-connected-devices-and-5g-should-push-that-even-higher-1203431225/*

[11] *https://www.zdnet.com/article/cybersecurity-these-are-the-internet-of-things-devices-that-are-most-targeted-by-hackers/*

[12] *https://safeatlast.co/blog/cybercrime-statistics/#gref*

[13] *https://hotforsecurity.bitdefender.com/blog/lack-of-awareness-leaves-consumers-vulnerable-to-cyberattacks-study-finds-20479.html*

Contact Us

sales@blackcloak.io

company/blackcloak

blackcloak.io

@BlackCloakCyber