Cyber Security for High Net-Worth Individuals

Meet Your Instructor

Hey there! This is Bill Weber, founder of Cyber Foundry.

I created this program to help High Net Worth Individuals get a better view into the risk that Information Technology can play in their personal lives by looking at some of the common problems we all face with outdated, insecure technology and some of the privacy intrusions that threaten us all.

Only after I "zoomed out" and created the Field Guide to Cybersecurity Best Practices, which covers many common tools to improve personal security, did I get a cohesive picture of how much our personal cyber hygiene really can affect us.

And the results were crazy…

Once I started looking at how my clients were exposed in their personal lives, I truly understood the nature of the problem. This is why this content is, and will always be, entirely free. Please take the content and pick your own adventure to challenge your own challenges in your personal IT life.

Understanding Your Risk

We assume the following:

- Your risk is higher than the average person because you are either a public figure, are of high net worth, or both.
- You are not being specifically targeted by an advanced, persistent, or well-funded adversary.
- Your goal is to understand your risk so that you can reduce as much it with the least effort possible.

I’m your best friend. I’m Santa Clause.
Don’t you want to be my best friend?

CASE STUDY

The Video Camera in this child’s room was hacked.

The criminal could watch and talk with the child whenever she was in her room because the camera had insecure default settings that the owner didn’t change.

Why Some Users Fail to Maintain Good Cyber Hygiene

- Leaders are wary of unquantified outcomes.
- Requires technical specialization.
- Identifying specific risks can be elusive.
- Security always seems to break productivity.

Is it raining,
or are you a target?

The more reasons you have to protect your privacy, the more incentives criminals have to target you.

This program helps High-net-worth individuals quickly reduce their personal risk from cyber criminals without the uncertainty and time commitment so they can protect their families and businesses.

Implement our recommendations, and we can demonstrate the reduction of risk to you and your family.

DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

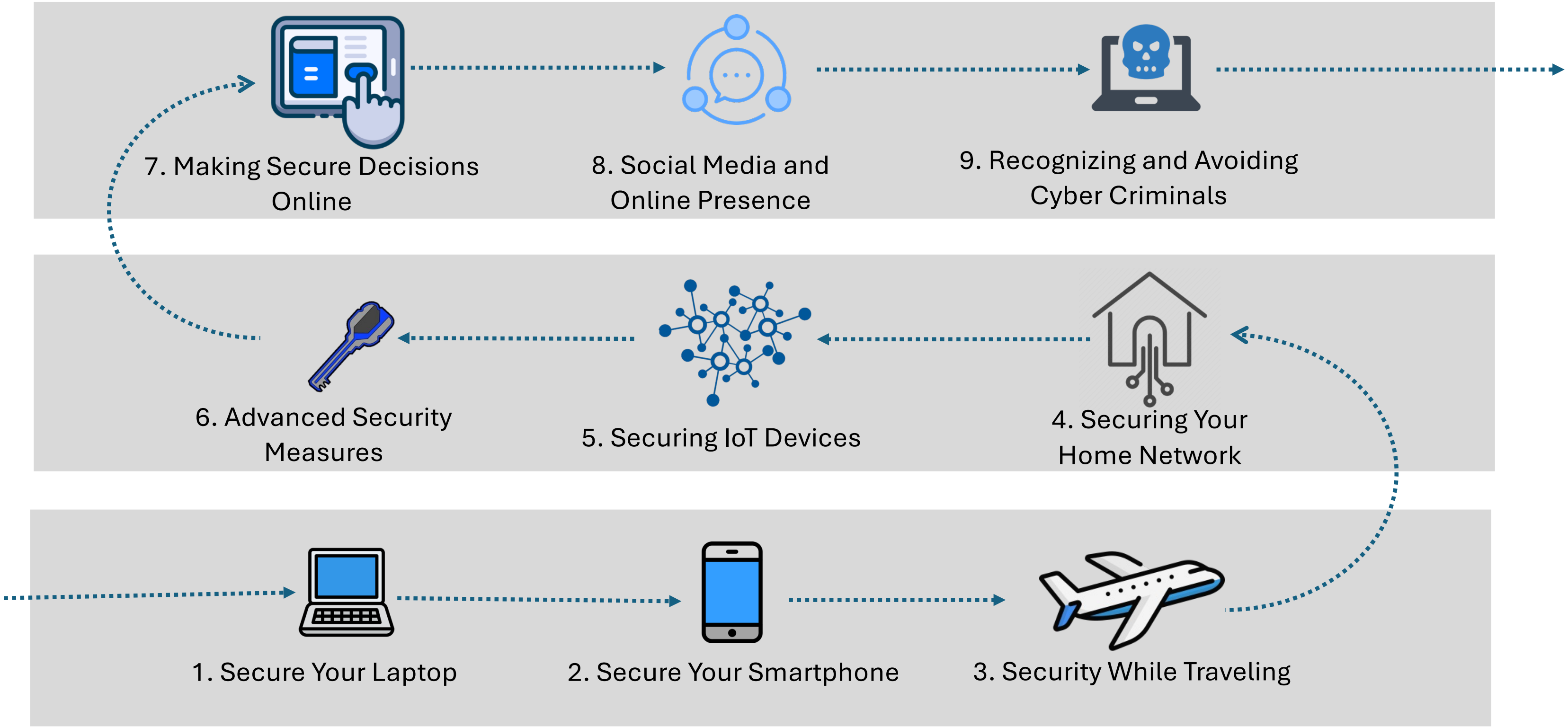
The largest vulnerabilities arise from forgetting the basics.

We provide simple cheat sheets that you and your team can use to keep you on track.

We reduce the most risk…
with the least effort…
By avoiding the most common Problems.

the 9 things you can do today to protect your family and business

Cybersecurity Best Practices Roadmap



1. Secure Your Laptop

2. Secure Your Smartphone

3. Security While Traveling

4. Securing Your Home Network

5. Securing IoT Devices

6. Advanced Security Measures

7. Making Secure Decisions Online

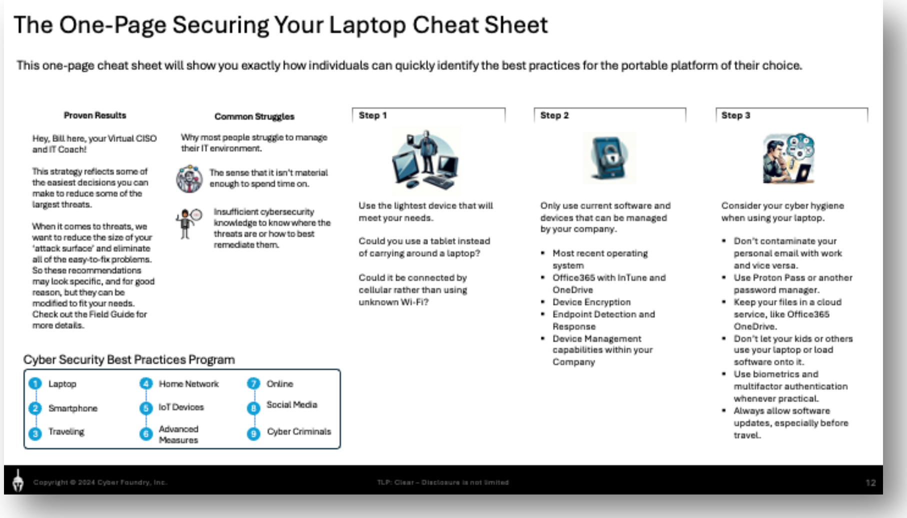
8. Social Media and Online Presence

9. Recognizing and Avoiding Cyber Criminals

Laptop Computers

Your Laptop = Single Stop Security Vulnerability

The most effective wat to improve your security is to reduce the scope and improve the quality.



The One-Page Securing Your Laptop Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices for the portable platform of their choice.

Proven Results

Hey, Bill here, your Virtual CISO and IT Coach!

This strategy reflects some of the easiest decisions you can make to reduce some of the largest threats.

When it comes to threats, we want to reduce the size of your 'attack surface' and eliminate all of the easy-to-fix problems. So these recommendations may look specific, and for good reason, but they can be modified to fit your needs. Check out the Field Guide for more details.

Common Struggles

Why most people struggle to manage their IT environment.

The sense that it isn't material enough to spend time on.

Insufficient cybersecurity knowledge to know where the threats are or how to best remediate them.

Step 1

Use the lightest device that will meet your needs.

Could you use a tablet instead of carrying around a laptop?

Could it be connected by cellular rather than using unknown Wi-Fi?

Step 2

Only use current software and devices that can be managed by your company.

- Most recent operating system
- Office365 with InTune and OneDrive
- Device Encryption
- Endpoint Detection and Response
- Device Management capabilities within your Company

Step 3

Consider your cyber hygiene when using your laptop.

- Don't contaminate your personal email with work and vice versa.
- Use Proton Pass or another password manager.
- Keep your files in a cloud service, like Office365 OneDrive.
- Don't let your kids or others use your laptop or load software onto it.
- Use biometrics and multifactor authentication whenever practical.
- Always allow software updates, especially before travel.

Cyber Security Best Practices Program

1 Laptop
2 Smartphone
3 Traveling
4 Home Network
5 IoT Devices
6 Advanced Measures
7 Online
8 Social Media
9 Cyber Criminals

Copyright © 2024 Cyber Foundry, Inc. TLP: Clear – Disclosure is not limited 12

The One-Page Securing Your Laptop Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices for the portable platform of their choice.

Proven Results

Hey, Bill here, your Virtual CISO and IT Coach!

This strategy reflects some of the easiest decisions you can make to reduce some of the largest threats.

When it comes to threats, we want to reduce the size of your ‘attack surface’ and eliminate all of the easy-to-fix problems. So these recommendations may look specific, and for good reason, but they can be modified to fit your needs. Check out the Field Guide for more details.

Common Struggles

Why most people struggle to manage their IT environment.

The sense that it isn’t material enough to spend time on.

Insufficient cybersecurity knowledge to know where the threats are or how to best remediate them.

Step 1

Use the lightest device that will meet your needs.

Could you use a tablet instead of carrying around a laptop?

Could it be connected by cellular rather than using unknown Wi-Fi?

Step 2

Only use current software and devices that can be managed by your company.

- Most recent operating system
- Office365 with InTune and OneDrive
- Device Encryption
- Endpoint Detection and Response
- Device Management capabilities within your Company

Step 3

Consider your cyber hygiene when using your laptop.

- Don’t contaminate your personal email with work and vice versa.
- Use Proton Pass or another password manager.
- Keep your files in a cloud service, like Office365 OneDrive.
- Don’t let your kids or others use your laptop or load software onto it.
- Use biometrics and multifactor authentication whenever practical.
- Always allow software updates, especially before travel.

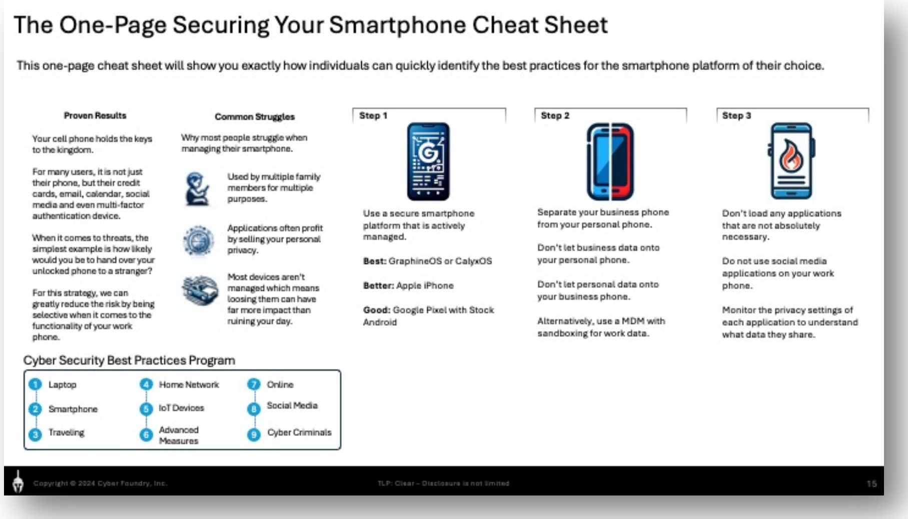
Cyber Security Best Practices Program

1 Laptop
2 Smartphone
3 Traveling
4 Home Network
5 IoT Devices
6 Advanced Measures
7 Online
8 Social Media
9 Cyber Criminals

Smartphones

Your phone knows more about you than your family

The best way to protect your privacy is to not openly share it with anyone who offers something pretty.



The One-Page Securing Your Smartphone Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices for the smartphone platform of their choice.

Proven Results

Your cell phone holds the keys to the kingdom.

For many users, it is not just their phone, but their credit cards, email, calendar, social media and even multi-factor authentication device.

When it comes to threats, the simplest example is how likely would you be to hand over your unlocked phone to a stranger?

For this strategy, we can greatly reduce the risk by being selective when it comes to the functionality of your work phone.

Common Struggles

Why most people struggle when managing their smartphone.

Used by multiple family members for multiple purposes.

Applications often profit by selling your personal privacy.

Most devices aren't managed which means loosing them can have far more impact than ruining your day.

Step 1

Use a secure smartphone platform that is actively managed.

Best: GraphineOS or CalyxOS

Better: Apple iPhone

Good: Google Pixel with Stock Android

Step 2

Separate your business phone from your personal phone.

Don't let business data onto your personal phone.

Don't let personal data onto your business phone.

Alternatively, use a MDM with sandboxing for work data.

Step 3

Don't load any applications that are not absolutely necessary.

Do not use social media applications on your work phone.

Monitor the privacy settings of each application to understand what data they share.

Cyber Security Best Practices Program

1 Laptop
2 Smartphone
3 Traveling
4 Home Network
5 IoT Devices
6 Advanced Measures
7 Online
8 Social Media
9 Cyber Criminals

TLP: Clear – Disclosure is not limited 15

The One-Page Securing Your Smartphone Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices for the smartphone platform of their choice.

Proven Results

Your cell phone holds the keys to the kingdom.

For many users, it is not just their phone, but their credit cards, email, calendar, social media and even multi-factor authentication device.

When it comes to threats, the simplest example is how likely would you be to hand over your unlocked phone to a stranger?

For this strategy, we can greatly reduce the risk by being selective when it comes to the functionality of your work phone.

Common Struggles

Why most people struggle when managing their smartphone.

Used by multiple family members for multiple purposes.

Applications often profit by selling your personal privacy.

Most devices aren't managed which means loosing them can have far more impact than ruining your day.

Step 1

Use a secure smartphone platform that is actively managed.

Best: GraphineOS or CalyxOS

Better: Apple iPhone

Good: Google Pixel with Stock Android

Step 2

Separate your business phone from your personal phone.

Don't let business data onto your personal phone.

Don't let personal data onto your business phone.

Alternatively, use a MDM with sandboxing for work data.

Step 3

Don't load any applications that are not absolutely necessary.

Do not use social media applications on your work phone.

Monitor the privacy settings of each application to understand what data they share.

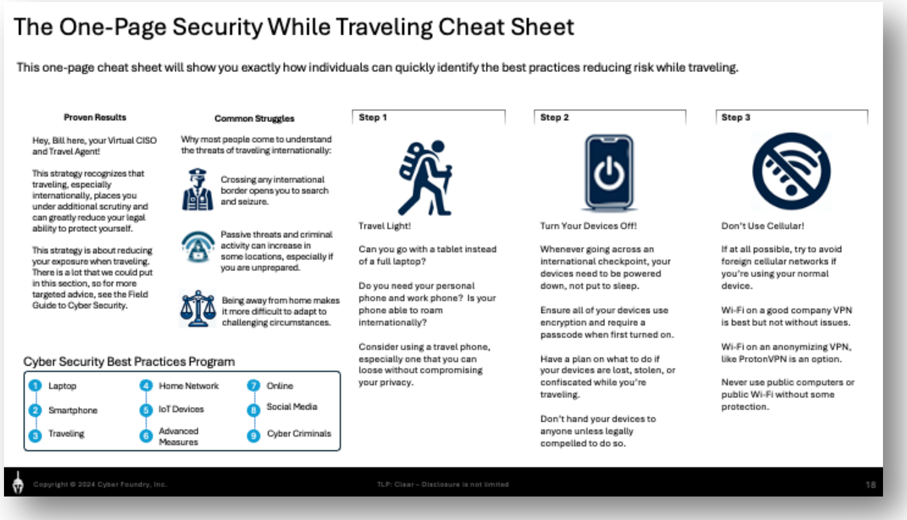
Cyber Security Best Practices Program

1. Laptop
2. Smartphone
3. Traveling
4. Home Network
5. IoT Devices
6. Advanced Measures
7. Online
8. Social Media
9. Cyber Criminals

Traveling

Your privacy is never more challenged than when crossing the border.

If you know your rights are significantly limited, the best strategy is to limit your exposure.



The One-Page Security While Traveling Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices reducing risk while traveling.

Proven Results

Hey, Bill here, your Virtual CISO and Travel Agent!

This strategy recognizes that traveling, especially internationally, places you under additional scrutiny and can greatly reduce your legal ability to protect yourself.

This strategy is about reducing your exposure when traveling. There is a lot that we could put in this section, so for more targeted advice, see the Field Guide to Cyber Security.

Common Struggles

Why most people come to understand the threats of traveling internationally:

Crossing any international border opens you to search and seizure.

Passive threats and criminal activity can increase in some locations, especially if you are unprepared.

Being away from home makes it more difficult to adapt to challenging circumstances.

Step 1

Travel Light!

Can you go with a tablet instead of a full laptop?

Do you need your personal phone and work phone? Is your phone able to roam internationally?

Consider using a travel phone, especially one that you can loose without compromising your privacy.

Step 2

Turn Your Devices Off!

Whenever going across an international checkpoint, your devices need to be powered down, not put to sleep.

Ensure all of your devices use encryption and require a passcode when first turned on.

Have a plan on what to do if your devices are lost, stolen, or confiscated while you're traveling.

Don't hand your devices to anyone unless legally compelled to do so.

Step 3

Don't Use Cellular!

If at all possible, try to avoid foreign cellular networks if you're using your normal device.

Wi-Fi on a good company VPN is best but not without issues.

Wi-Fi on an anonymizing VPN, like ProtonVPN is an option.

Never use public computers or public Wi-Fi without some protection.

Cyber Security Best Practices Program

1. Laptop
2. Smartphone
3. Traveling
4. Home Network
5. IoT Devices
6. Advanced Measures
7. Online
8. Social Media
9. Cyber Criminals

TLP: Clear – Disclosure is not limited

18

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."
-Edward Snowden

The One-Page Security While Traveling Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices reducing risk while traveling.

Proven Results

Hey, Bill here, your Virtual CISO and Travel Agent!

This strategy recognizes that traveling, especially internationally, places you under additional scrutiny and can greatly reduce your legal ability to protect yourself.

This strategy is about reducing your exposure when traveling. There is a lot that we could put in this section, so for more targeted advice, see the Field Guide to Cyber Security.

Common Struggles

Why most people come to understand the threats of traveling internationally:

Crossing any international border opens you to search and seizure.

Passive threats and criminal activity can increase in some locations, especially if you are unprepared.

Being away from home makes it more difficult to adapt to challenging circumstances.

Cyber Security Best Practices Program

1. Laptop
2. Smartphone
3. Traveling
4. Home Network
5. IoT Devices
6. Advanced Measures
7. Online
8. Social Media
9. Cyber Criminals

Step 1

Travel Light!

Can you go with a tablet instead of a full laptop?

Do you need your personal phone and work phone? Is your phone able to roam internationally?

Consider using a travel phone, especially one that you can loose without compromising your privacy.

Step 2

Turn Your Devices Off!

Whenever going across an international checkpoint, your devices need to be powered down, not put to sleep.

Ensure all of your devices use encryption and require a passcode when first turned on.

Have a plan on what to do if your devices are lost, stolen, or confiscated while you're traveling.

Don't hand your devices to anyone unless legally compelled to do so.

Step 3

Don't Use Cellular!

If at all possible, try to avoid foreign cellular networks if you're using your normal device.

Wi-Fi on a good company VPN is best but not without issues.

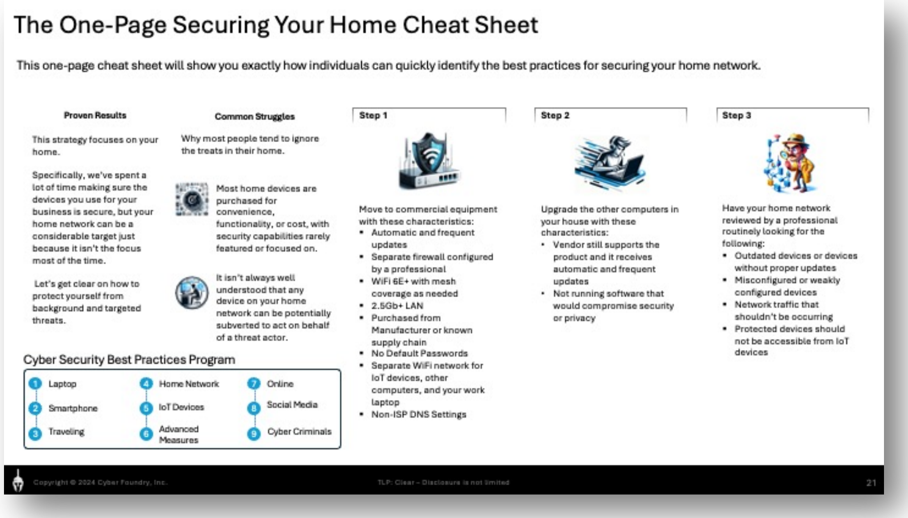
Wi-Fi on an anonymizing VPN, like ProtonVPN is an option.

Never use public computers or public Wi-Fi without some protection.

Home

Your home may be the single largest threat to your security.

Taking your highly secured laptop into an environment where there is usually no security significantly raises your risk.



The One-Page Securing Your Home Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices for securing your home network.

Proven Results

This strategy focuses on your home.

Specifically, we've spent a lot of time making sure the devices you use for your business is secure, but your home network can be a considerable target just because it isn't the focus most of the time.

Let's get clear on how to protect yourself from background and targeted threats.

Common Struggles

Why most people tend to ignore the treats in their home.

Most home devices are purchased for convenience, functionality, or cost, with security capabilities rarely featured or focused on.

It isn't always well understood that any device on your home network can be potentially subverted to act on behalf of a threat actor.

Cyber Security Best Practices Program

1. Laptop
2. Smartphone
3. Traveling
4. Home Network
5. IoT Devices
6. Advanced Measures
7. Online
8. Social Media
9. Cyber Criminals

Step 1

Move to commercial equipment with these characteristics:

- Automatic and frequent updates
- Separate firewall configured by a professional
- WiFi 6E+ with mesh coverage as needed
- 2.5Gb+ LAN
- Purchased from Manufacturer or known supply chain
- No Default Passwords
- Separate WiFi network for IoT devices, other computers, and your work laptop
- Non-ISP DNS Settings

Step 2

Upgrade the other computers in your house with these characteristics:

- Vendor still supports the product and it receives automatic and frequent updates
- Not running software that would compromise security or privacy

Step 3

Have your home network reviewed by a professional routinely looking for the following:

- Outdated devices or devices without proper updates
- Misconfigured or weakly configured devices
- Network traffic that shouldn't be occurring
- Protected devices should not be accessible from IoT devices

Copyright © 2024 Cyber Foundry, Inc.

TLP: Clear – Disclosure is not limited

21

The One-Page Securing Your Home Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices for securing your home network.

Proven Results

This strategy focuses on your home.

Specifically, we've spent a lot of time making sure the devices you use for your business is secure, but your home network can be a considerable target just because it isn't the focus most of the time.

Let's get clear on how to protect yourself from background and targeted threats.

Common Struggles

Why most people tend to ignore the treats in their home.

Most home network devices are purchased for convenience, cost, or functionality, with security capabilities rarely featured or focused on.

It isn't always well understood that any device on your home network can be potentially subverted to act on behalf of a threat actor.

Cyber Security Best Practices Program

1. Laptop
2. Smartphone
3. Traveling
4. Home Network
5. IoT Devices
6. Advanced Measures
7. Online
8. Social Media
9. Cyber Criminals

Step 1

Move to commercial equipment with these characteristics:

- Automatic and frequent updates
- Separate firewall configured by a professional
- WiFi 6E+ with mesh coverage as needed
- 2.5Gb+ LAN
- Purchased from Manufacturer or known supply chain
- No Default Passwords
- Separate WiFi network for IoT devices, other computers, and your work laptop
- Non-ISP DNS Settings

Step 2

Upgrade the other computers in your house with these characteristics:

- Vendor still supports the product and it receives automatic and frequent updates
- Not running software that would compromise security or privacy

Step 3

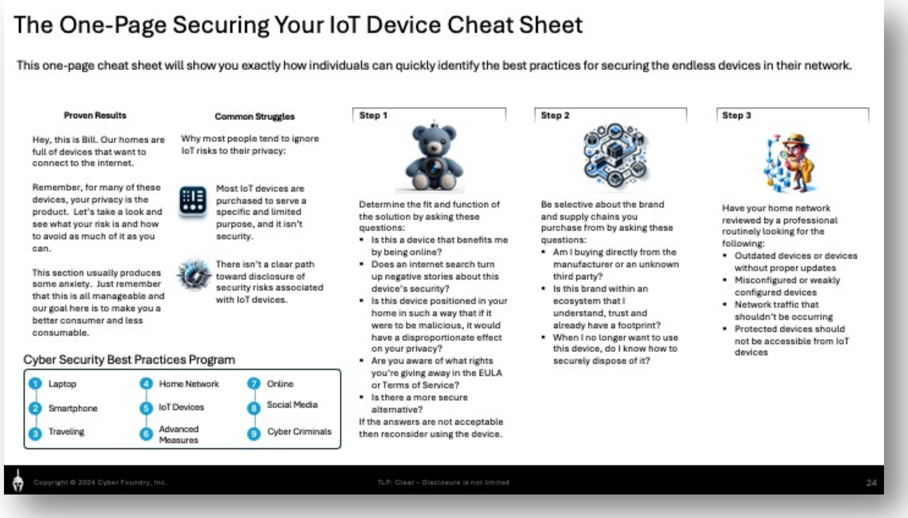
Have your home network reviewed by a professional routinely looking for the following:

- Outdated devices or devices without proper updates
- Misconfigured or weakly configured devices
- Network traffic that shouldn't be occurring
- Protected devices should not be accessible from IoT devices

Internet of Things (IoT)

Are your children's toys watching them?

Everything seems to be connected to the Internet, but why? Remember that your privacy and security is worth money, to many people.



The One-Page Securing Your IoT Device Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices for securing the endless devices in their network.

Proven Results

Hey, this is Bill. Our homes are full of devices that want to connect to the internet.

Remember, for many of these devices, your privacy is the product. Let's take a look and see what your risk is and how to avoid as much of it as you can.

This section usually produces some anxiety. Just remember that this is all manageable and our goal here is to make you a better consumer and less consumable.

Common Struggles

Why most people tend to ignore IoT risks to their privacy:

Most IoT devices are purchased to serve a specific and limited purpose, and it isn't security.

There isn't a clear path toward disclosure of security risks associated with IoT devices.

Step 1

Determine the fit and function of the solution by asking these questions:

- Is this a device that benefits me by being online?
- Does an internet search turn up negative stories about this device's security?
- Is this device positioned in your home in such a way that if it were to be malicious, it would have a disproportionate effect on your privacy?
- Are you aware of what rights you're giving away in the EULA or Terms of Service?
- Is there a more secure alternative?

If the answers are not acceptable then reconsider using the device.

Step 2

Be selective about the brand and supply chains you purchase from by asking these questions:

- Am I buying directly from the manufacturer or an unknown third party?
- Is this brand within an ecosystem that I understand, trust and already have a footprint?
- When I no longer want to use this device, do I know how to securely dispose of it?

Step 3

Have your home network reviewed by a professional routinely looking for the following:

- Outdated devices or devices without proper updates
- Misconfigured or weakly configured devices
- Network traffic that shouldn't be occurring
- Protected devices should not be accessible from IoT devices

Cyber Security Best Practices Program

1 Laptop
2 Smartphone
3 Traveling
4 Home Network
5 IoT Devices
6 Advanced Measures
7 Online
8 Social Media
9 Cyber Criminals

Copyright © 2024 Cyber Foundry, Inc. TLP: Clear – Disclosure is not limited 24

The One-Page Securing Your IoT Device Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices for securing the endless devices in their network.

Proven Results

Hey, this is Bill. Our homes are full of devices that want to connect to the internet.

Remember, for many of these devices, your privacy is the product. Let's take a look and see what your risk is and how to avoid as much of it as you can.

This section usually produces some anxiety. Just remember that this is all manageable and our goal here is to make you a better consumer and less consumable.

Common Struggles

Why most people tend to ignore IoT risks to their privacy:

Most IoT devices are purchased to serve a specific and limited purpose, and it isn't security.

There isn't a clear path toward disclosure of security risks associated with IoT devices.

Cyber Security Best Practices Program

1 Laptop
2 Smartphone
3 Traveling
4 Home Network
5 IoT Devices
6 Advanced Measures
7 Online
8 Social Media
9 Cyber Criminals

Step 1

Determine the fit and function of the solution by asking these questions:

- Is this a device that benefits me by being online?
- Does an internet search turn up negative stories about this device's security?
- Is this device positioned in your home in such a way that if it were to be malicious, it would have a disproportionate effect on your privacy?
- Are you aware of what rights you're giving away in the EULA or Terms of Service?
- Is there a more secure alternative?

If the answers are not acceptable then reconsider using the device.

Step 2

Be selective about the brand and supply chains you purchase from by asking these questions:

- Am I buying directly from the manufacturer or an unknown third party?
- Is this brand within an ecosystem that I understand, trust and already have a footprint?
- When I no longer want to use this device, do I know how to securely dispose of it?

Step 3

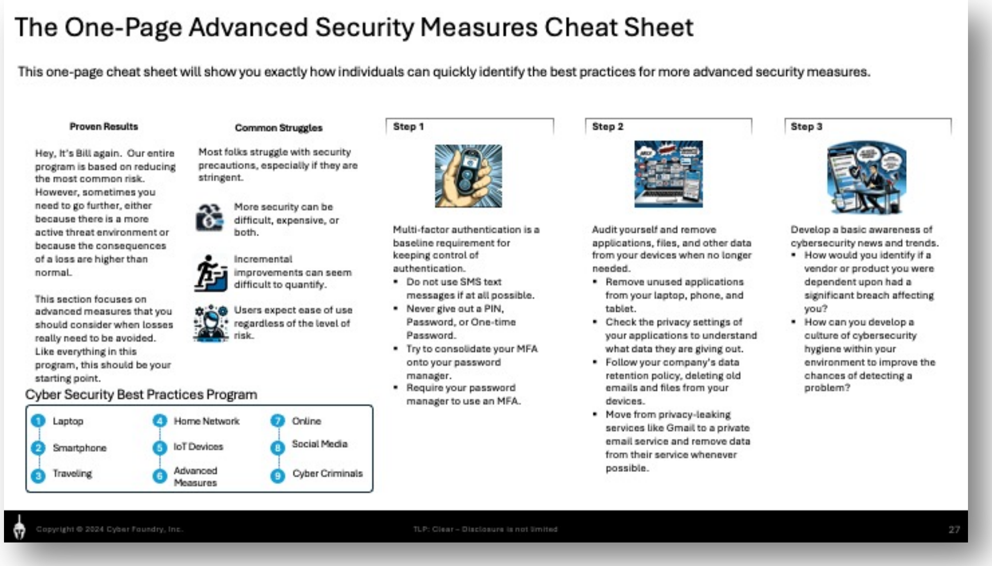
Have your home network reviewed by a professional routinely looking for the following:

- Outdated devices or devices without proper updates
- Misconfigured or weakly configured devices
- Network traffic that shouldn't be occurring
- Protected devices should not be accessible from IoT devices

Advanced Measures

Remember not all risks are equal

Sometimes you will need a little protection, and sometimes you will need more advanced capabilities.
Can you tell the difference?



The One-Page Advanced Security Measures Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices for more advanced security measures.

Proven Results

Hey, It's Bill again. Our entire program is based on reducing the most common risk. However, sometimes you need to go further, either because there is a more active threat environment or because the consequences of a loss are higher than normal.

This section focuses on advanced measures that you should consider when losses really need to be avoided. Like everything in this program, this should be your starting point.

Common Struggles

Most folks struggle with security precautions, especially if they are stringent.

More security can be difficult, expensive, or both.

Incremental improvements can seem difficult to quantify.

Users expect ease of use regardless of the level of risk.

Step 1

Multi-factor authentication is a baseline requirement for keeping control of authentication.

- Do not use SMS text messages if at all possible.
- Never give out a PIN, Password, or One-time Password.
- Try to consolidate your MFA onto your password manager.
- Require your password manager to use an MFA.

Step 2

Audit yourself and remove applications, files, and other data from your devices when no longer needed.

- Remove unused applications from your laptop, phone, and tablet.
- Check the privacy settings of your applications to understand what data they are giving out.
- Follow your company's data retention policy, deleting old emails and files from your devices.
- Move from privacy-leaking services like Gmail to a private email service and remove data from their service whenever possible.

Step 3

Develop a basic awareness of cybersecurity news and trends.

- How would you identify if a vendor or product you were dependent upon had a significant breach affecting you?
- How can you develop a culture of cybersecurity hygiene within your environment to improve the chances of detecting a problem?

Cyber Security Best Practices Program

1 Laptop
2 Smartphone
3 Traveling
4 Home Network
5 IoT Devices
6 Advanced Measures
7 Online
8 Social Media
9 Cyber Criminals

Copyright © 2024 Cyber Foundry, Inc. TLP: Clear – Disclosure is not limited 27

The One-Page Advanced Security Measures Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices for more advanced security measures.

Proven Results

Hey, It's Bill again. Our entire program is based on reducing the most common risk. However, sometimes you need to go further, either because there is a more active threat environment or because the consequences of a loss are higher than normal.

This section focuses on advanced measures that you should consider when losses really need to be avoided. Like everything in this program, this should be your starting point.

Common Struggles

Most folks struggle with security precautions, especially if they are stringent.

More security can be difficult, expensive, or both.

Incremental improvements can seem difficult to quantify.

Users expect ease of use regardless of the level of risk.

Step 1

Multi-factor authentication is a baseline requirement for keeping control of authentication.

- Do not use SMS text messages if at all possible.
- Never give out a PIN, Password, or One-time Password.
- Try to consolidate your MFA onto your password manager.
- Require your password manager to use an MFA.

Step 2

Audit yourself and remove applications, files, and other data from your devices when no longer needed.

- Remove unused applications from your laptop, phone, and tablet.
- Check the privacy settings of your applications to understand what data they are giving out.
- Follow your company's data retention policy, deleting old emails and files from your devices.
- Move from privacy-leaking services like Gmail to a private email service and remove data from their service whenever possible.

Step 3

Develop a basic awareness of cybersecurity news and trends.

- How would you identify if a vendor or product you were dependent upon had a significant breach affecting you?
- How can you develop a culture of cybersecurity hygiene within your environment to improve the chances of detecting a problem?

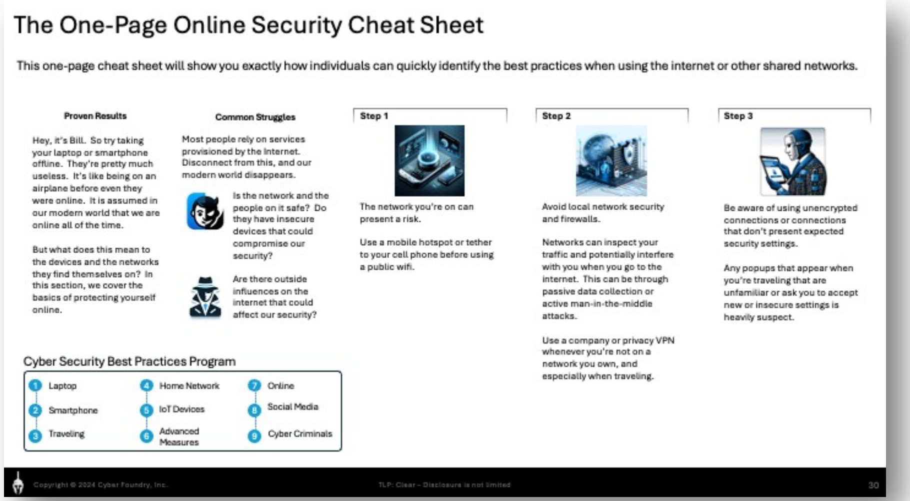
Cyber Security Best Practices Program

1 Laptop
2 Smartphone
3 Traveling
4 Home Network
5 IoT Devices
6 Advanced Measures
7 Online
8 Social Media
9 Cyber Criminals

Online Security

Securing yourself while online

Most devices are only useful when online. What does that mean to your ongoing security?



The One-Page Online Security Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices when using the internet or other shared networks.

Proven Results

Hey, it's Bill. So try taking your laptop or smartphone offline. They're pretty much useless. It's like being on an airplane before even they were online. It is assumed in our modern world that we are online all of the time.

But what does this mean to the devices and the networks they find themselves on? In this section, we cover the basics of protecting yourself online.

Common Struggles

Most people rely on services provisioned by the Internet. Disconnect from this, and our modern world disappears.

Is the network and the people on it safe? Do they have insecure devices that could compromise our security?

Are there outside influences on the internet that could affect our security?

Step 1

The network you're on can present a risk.

Use a mobile hotspot or tether to your cell phone before using a public wifi.

Step 2

Avoid local network security and firewalls.

Networks can inspect your traffic and potentially interfere with you when you go to the internet. This can be through passive data collection or active man-in-the-middle attacks.

Use a company or privacy VPN whenever you're not on a network you own, and especially when traveling.

Step 3

Be aware of using unencrypted connections or connections that don't present expected security settings.

Any popups that appear when you're traveling that are unfamiliar or ask you to accept new or insecure settings is heavily suspect.

Cyber Security Best Practices Program

1. Laptop
2. Smartphone
3. Traveling
4. Home Network
5. IoT Devices
6. Advanced Measures
7. Online
8. Social Media
9. Cyber Criminals

Copyright © 2024 Cyber Foundry, Inc. TLP: Clear – Disclosure is not limited 30

The One-Page Online Security Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices when using the internet or other shared networks.

Proven Results

Hey, it's Bill. So try taking your laptop or smartphone offline. They're pretty much useless. It's like being on an airplane before even they were online. It is assumed in our modern world that we are online all of the time.

But what does this mean to the devices and the networks they find themselves on? In this section, we cover the basics of protecting yourself online.

Common Struggles

Most people rely on services provisioned by the Internet. Disconnect from this, and our modern world disappears.

Is the network and the people on it safe? Do they have insecure devices that could compromise our security?

Are there outside influences on the internet that could affect our security?

Step 1

The network you're on can present a risk.

Use a mobile hotspot or tether to your cell phone before using a public wifi.

Step 2

Avoid local network security and firewalls.

Networks can inspect your traffic and potentially interfere with you when you go to the internet. This can be through passive data collection or active man-in-the-middle attacks.

Use a company or privacy VPN whenever you're not on a network you own, and especially when traveling.

Step 3

Be aware of using unencrypted connections or connections that don't present expected security settings.

Any popups that appear when you're traveling that are unfamiliar or ask you to accept new or insecure settings is heavily suspect.

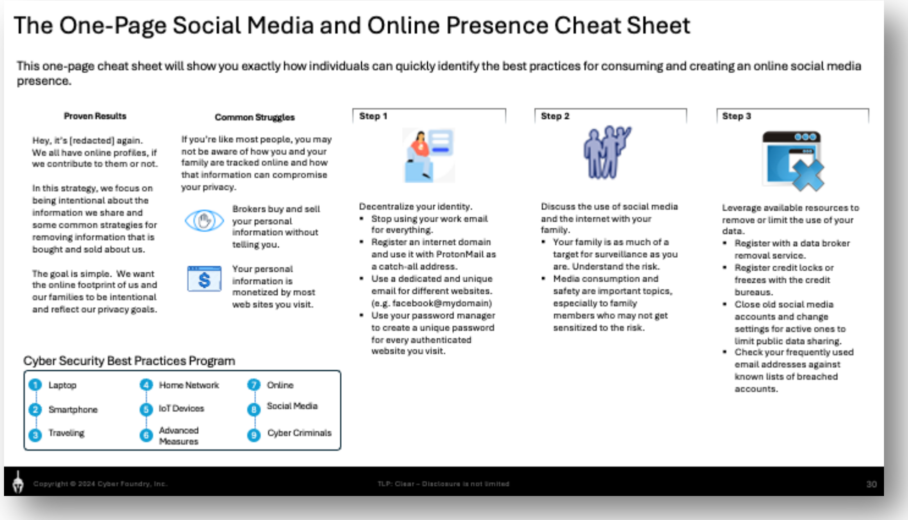
Cyber Security Best Practices Program

1 Laptop
2 Smartphone
3 Traveling
4 Home Network
5 IoT Devices
6 Advanced Measures
7 Online
8 Social Media
9 Cyber Criminals

Social Media / Online Presence

Locking Down Your Likes: Shielding Social Media from Cyber Criminals

Building a safer digital identity amidst likes and links.



The One-Page Social Media and Online Presence Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices for consuming and creating an online social media presence.

Proven Results

Hey, it's [redacted] again. We all have online profiles, if we contribute to them or not.

In this strategy, we focus on being intentional about the information we share and some common strategies for removing information that is bought and sold about us.

The goal is simple. We want the online footprint of us and our families to be intentional and reflect our privacy goals.

Common Struggles

If you're like most people, you may not be aware of how you and your family are tracked online and how that information can compromise your privacy.

Brokers buy and sell your personal information without telling you.

Your personal information is monetized by most web sites you visit.

Step 1

Decentralize your identity.

- Stop using your work email for everything.
- Register an internet domain and use it with ProtonMail as a catch-all address.
- Use a dedicated and unique email for different websites. (e.g. facebook@mydomain)
- Use your password manager to create a unique password for every authenticated website you visit.

Step 2

Discuss the use of social media and the internet with your family.

- Your family is as much of a target for surveillance as you are. Understand the risk.
- Media consumption and safety are important topics, especially to family members who may not get sensitized to the risk.

Step 3

Leverage available resources to remove or limit the use of your data.

- Register with a data broker removal service.
- Register credit locks or freezes with the credit bureaus.
- Close old social media accounts and change settings for active ones to limit public data sharing.
- Check your frequently used email addresses against known lists of breached accounts.

Cyber Security Best Practices Program

1 Laptop	4 Home Network	7 Online
2 Smartphone	5 IoT Devices	8 Social Media
3 Traveling	6 Advanced Measures	9 Cyber Criminals

Copyright © 2024 Cyber Foundry, Inc. TLP: Clear – Disclosure is not limited 30

The One-Page Social Media and Online Presence Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify the best practices for consuming and creating an online social media presence.

Proven Results

Hey, it's [redacted] again. We all have online profiles, if we contribute to them or not.

In this strategy, we focus on being intentional about the information we share and some common strategies for removing information that is bought and sold about us.

The goal is simple. We want the online footprint of us and our families to be intentional and reflect our privacy goals.

Common Struggles

If you're like most people, you may not be aware of how you and your family are tracked online and how that information can compromise your privacy.

Brokers buy and sell your personal information without telling you.

Your personal information is monetized by most web sites you visit.

Cyber Security Best Practices Program

1 Laptop
2 Smartphone
3 Traveling
4 Home Network
5 IoT Devices
6 Advanced Measures
7 Online
8 Social Media
9 Cyber Criminals

Step 1

Decentralize your identity.

- Stop using your work email for everything.
- Register an internet domain and use it with ProtonMail as a catch-all address.
- Use a dedicated and unique email for different websites. (e.g. facebook@mydomain)
- Use your password manager to create a unique password for every authenticated website you visit.

Step 2

Discuss the use of social media and the internet with your family.

- Your family is as much of a target for surveillance as you are. Understand the risk.
- Media consumption and safety are important topics, especially to family members who may not get sensitized to the risk.

Step 3

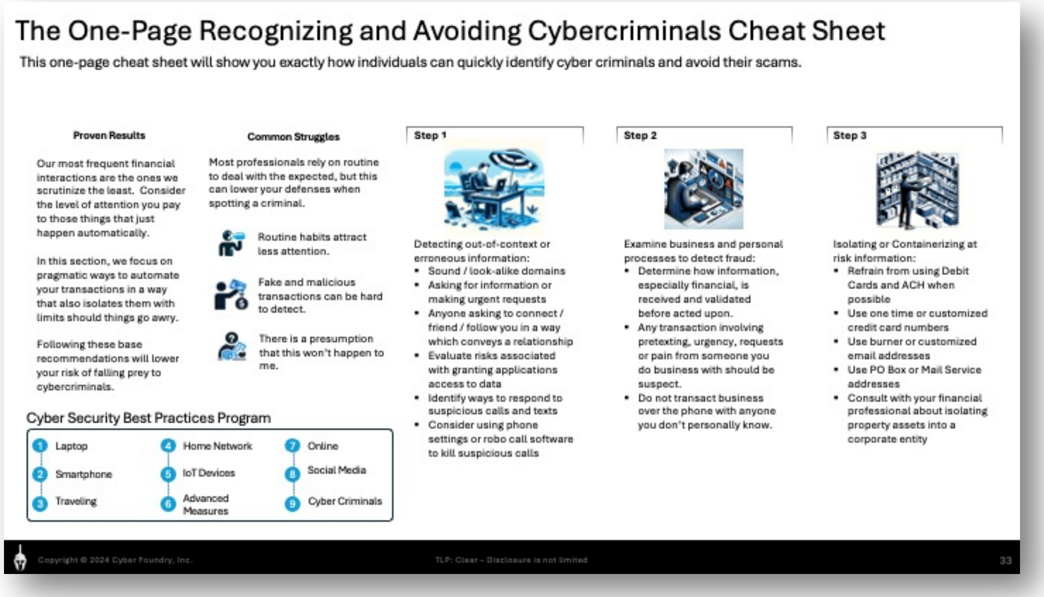
Leverage available resources to remove or limit the use of your data.

- Register with a data broker removal service.
- Register credit locks or freezes with the credit bureaus.
- Close old social media accounts and change settings for active ones to limit public data sharing.
- Check your frequently used email addresses against known lists of breached accounts.

Avoiding Cyber Criminals

On the Internet, Your Privacy and Security are Monetized

Sometimes by the 'free' products and services you use, sometimes by those who would steal your lunch.



The One-Page Recognizing and Avoiding Cybercriminals Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify cyber criminals and avoid their scams.

Proven Results

Our most frequent financial interactions are the ones we scrutinize the least. Consider the level of attention you pay to those things that just happen automatically.

In this section, we focus on pragmatic ways to automate your transactions in a way that also isolates them with limits should things go awry.

Following these base recommendations will lower your risk of falling prey to cybercriminals.

Common Struggles

Most professionals rely on routine to deal with the expected, but this can lower your defenses when spotting a criminal.

Routine habits attract less attention.

Fake and malicious transactions can be hard to detect.

There is a presumption that this won't happen to me.

Step 1

Detecting out-of-context or erroneous information:

- Sound / look-alike domains
- Asking for information or making urgent requests
- Anyone asking to connect / friend / follow you in a way which conveys a relationship
- Evaluate risks associated with granting applications access to data
- Identify ways to respond to suspicious calls and texts
- Consider using phone settings or robo call software to kill suspicious calls

Step 2

Examine business and personal processes to detect fraud:

- Determine how information, especially financial, is received and validated before acted upon.
- Any transaction involving pretexting, urgency, requests or pain from someone you do business with should be suspect.
- Do not transact business over the phone with anyone you don't personally know.

Step 3

Isolating or Containerizing at risk information:

- Refrain from using Debit Cards and ACH when possible
- Use one time or customized credit card numbers
- Use burner or customized email addresses
- Use PO Box or Mail Service addresses
- Consult with your financial professional about isolating property assets into a corporate entity

Cyber Security Best Practices Program

1. Laptop
2. Smartphone
3. Traveling
4. Home Network
5. IoT Devices
6. Advanced Measures
7. Online
8. Social Media
9. Cyber Criminals

Copyright © 2024 Cyber Foundry, Inc. TLP: Clear – Disclosure is not limited 33

The One-Page Recognizing and Avoiding Cybercriminals Cheat Sheet

This one-page cheat sheet will show you exactly how individuals can quickly identify cyber criminals and avoid their scams.

Proven Results

Our most frequent financial interactions are the ones we scrutinize the least. Consider the level of attention you pay to those things that just happen automatically.

In this section, we focus on pragmatic ways to automate your transactions in a way that also isolates them with limits should things go awry.

Following these base recommendations will lower your risk of falling prey to cybercriminals.

Common Struggles

Most professionals rely on routine to deal with the expected, but this can lower your defenses when spotting a criminal.

Routine habits attract less attention.

Fake and malicious transactions can be hard to detect.

There is a presumption that this won't happen to me.

Cyber Security Best Practices Program

1 Laptop
2 Smartphone
3 Traveling
4 Home Network
5 IoT Devices
6 Advanced Measures
7 Online
8 Social Media
9 Cyber Criminals

Step 1

Detecting out-of-context or erroneous information:

- Sound / look-alike domains
- Asking for information or making urgent requests
- Anyone asking to connect / friend / follow you in a way which conveys a relationship
- Evaluate risks associated with granting applications access to data
- Identify ways to respond to suspicious calls and texts
- Consider using phone settings or robo call software to kill suspicious calls

Step 2

Examine business and personal processes to detect fraud:

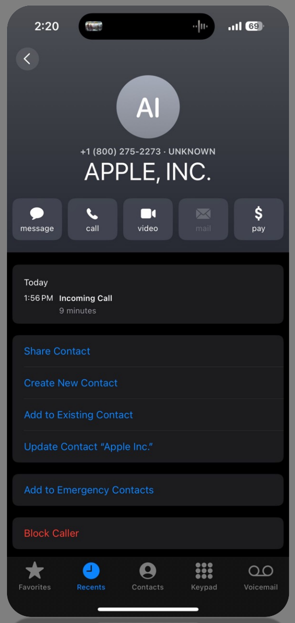
- Determine how information, especially financial, is received and validated before acted upon.
- Any transaction involving pretexting, urgency, requests or pain from someone you do business with should be suspect.
- Do not transact business over the phone with anyone you don't personally know.

Step 3

Isolating or Containerizing at risk information:

- Refrain from using Debit Cards and ACH when possible
- Use one time or customized credit card numbers
- Use burner or customized email addresses
- Use PO Box or Mail Service addresses
- Consult with your financial professional about isolating property assets into a corporate entity

Summary



2:20

AI

+1 (800) 275-2273 · UNKNOWN

APPLE, INC.

Today

1:56 PM Incoming Call

9 minutes

CASE STUDY

[I got a phone call today.] The caller ID said, "Apple, Inc." I answered.
Here's how it went:

An American-sounding individual identified himself as Eric with Apple support. He immediately said I can verify the number on "apple dot com slash contact."

He said he was calling me because someone had added a device and a phone number to my Apple account and had added a credit card to my Apple Pay. He confirmed he was calling from the #fraud department and mentioned that because of the "red flags," he was reaching out to me.

Eric asked if I had authorized the actions (adding a device, phone number, and credit card number). He said that the location was in Canada and he asked me if I wanted the phone number added, which he provided when I said, "yes" (514-887-2500).

He proceeded to lock my account, but in order for him to do that, he needed to send me a PIN so I could read it back to him. The PIN code I received contained the 6-digit code and a simple statement, "Do not share this with anyone." I began to press on why he needed the code in order to lock my account. He pushed back and then said I'd need to go to an Apple store to unlock it. (None of this makes sense because he needed the code to lock it but told me I needed to go in person to unlock my account.)

At the end of the call, I asked him for his ID which he provided me with an 8-digit number as well as a reference number that I'd need when I go to the Apple store.

CASE STUDY

Pretext

Urgency

Request

Pain

[I got a phone call today.] The caller ID said, "Apple, Inc." I answered.
Here's how it went:

An American-sounding individual identified himself as Eric with Apple support. He immediately said I can verify the number on "apple dot com slash contact."

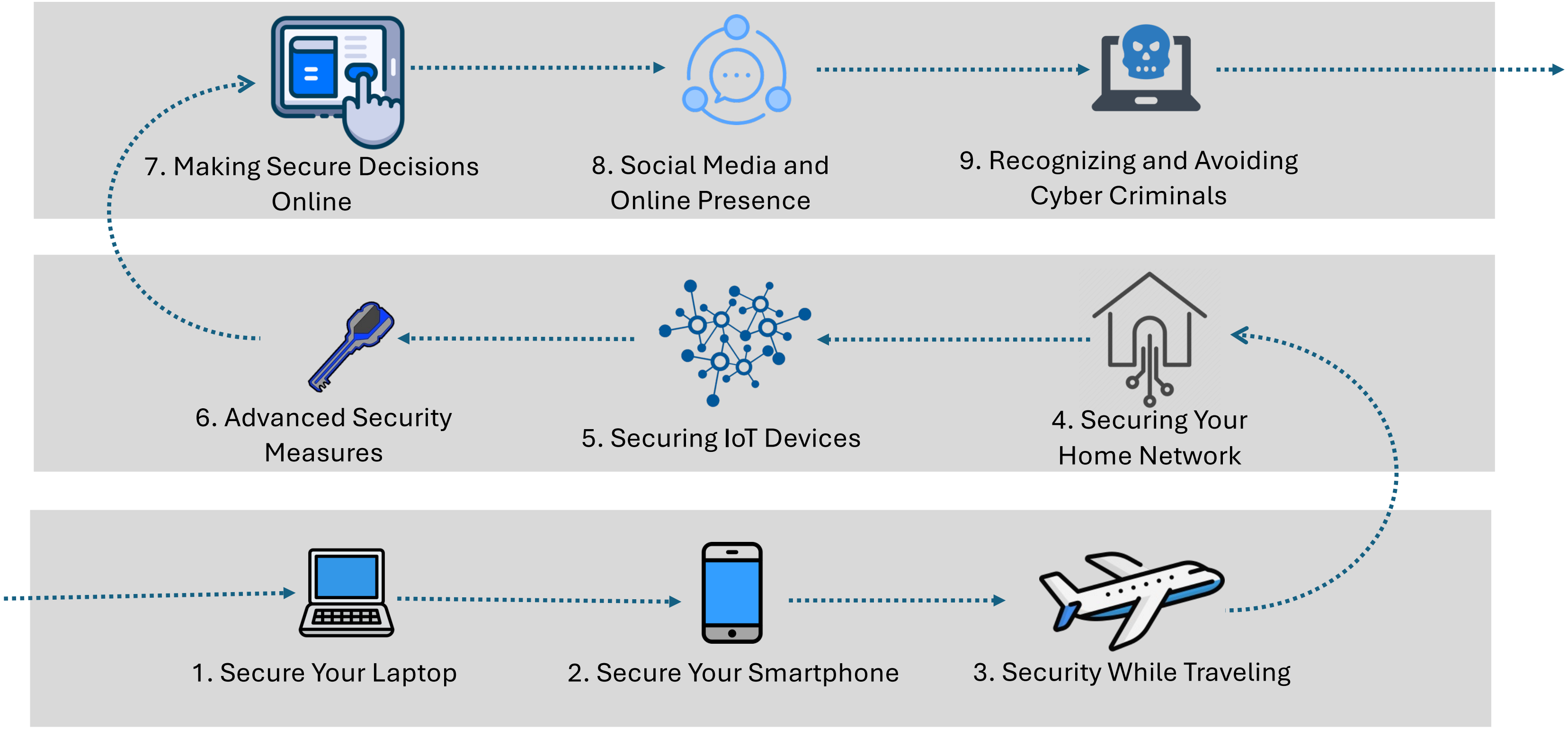
He said he was calling me because someone had added a device and a phone number to my Apple account and had added a credit card to my Apple Pay. He confirmed he was calling from the #fraud department and mentioned that because of the "red flags," he was reaching out to me.

Eric asked if I had authorized the actions (adding a device, phone number, and credit card number). He said that the location was in Canada and he asked me if I wanted the phone number added, which he provided when I said, "yes".

He proceeded to lock my account but in order for him to do that, he needed to send me a PIN so I could read it back to him. The PIN code I received contained the 6-digit code and a simple statement, ”Do not share this with anyone." I began to press on why he needed the code in order to lock my account. He pushed back and then said I'd need to go to an Apple store to unlock it. (None of this makes sense because he needed the code to lock it, but told me I needed go in-person to unlock my account.)

At the end of the call, I asked him for his ID which he provided me with an 8-digit number as well as a reference number that I'd need when I go to the Apple store.

Cybersecurity Best Practices Roadmap


7. Making Secure Decisions Online
8. Social Media and Online Presence
9. Recognizing and Avoiding Cyber Criminals
6. Advanced Security Measures
5. Securing IoT Devices
4. Securing Your Home Network
1. Secure Your Laptop
2. Secure Your Smartphone
3. Security While Traveling

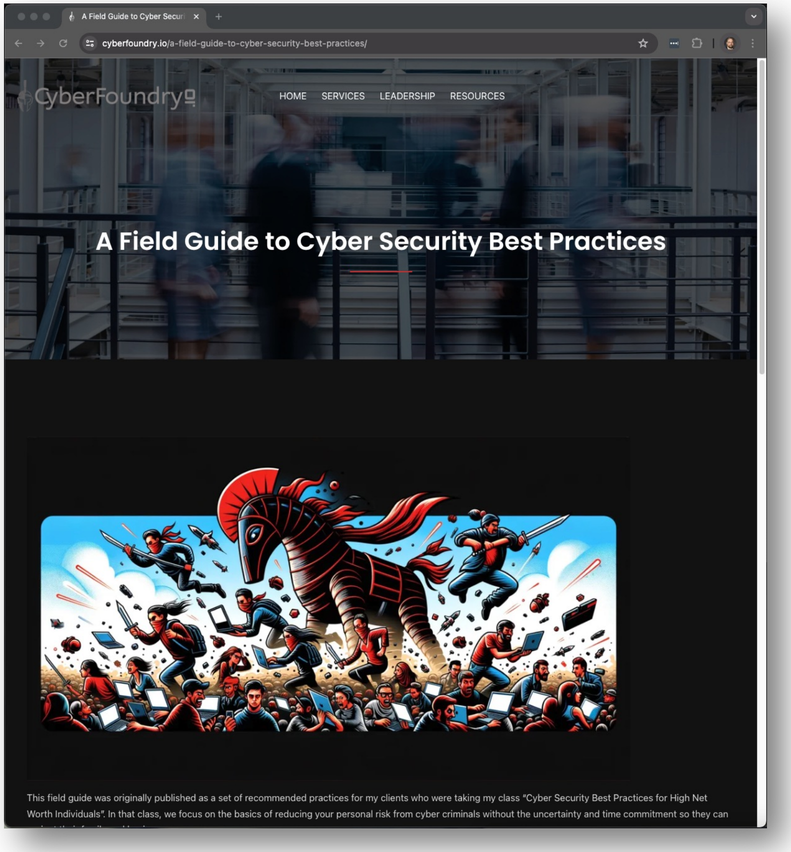
WARNING

Our Recommendations are Best Practices and therefore things you should do.

However, our recommendations are not sufficient by themselves.

Your Risk Is Unique

- Always Seek Professional Help
- Consider Any Solution Against Possible Losses


A Field Guide to Cyber Securi
cyberfoundry.io/a-field-guide-to-cyber-security-best-practices/
CyberFoundry
HOME
SERVICES
LEADERSHIP
RESOURCES

A Field Guide to Cyber Security Best Practices

This field guide was originally published as a set of recommended practices for my clients who were taking my class "Cyber Security Best Practices for High Net Worth Individuals". In that class, we focus on the basics of reducing your personal risk from cyber criminals without the uncertainty and time commitment so they can

Field Guide to Cybersecurity Best Practices

Once you get into the recommendations I make here, you may quickly come to the realization that it this can be complex and not all recommendations are equally beneficial.

Cybersecurity is, at its best, a complement to the business and technology use cases you individually have, so not all recommendations should be followed.

To this point, I've tried to give you checklists for categories of best practices that you should consider. To give these checklists more value, I've also created a web site called a Field Guide for Cybersecurity Best Practices.

This is a list of standard operating procedures for configurations and recommendations from the time they were written.

This isn't the kind of website you'll ever read in its entirety.
Your IT folk can look at it for more specific information on the recommendations I've made here. I hope you and they find it helpful as you work to reduce the real world threats out there.

If at the end of the day you want a more focused conversation on your risk and how we can manage it together, give me a call.

https://www.cyberfoundry.io/a-field-guide-to-cyber-security-best-practices/