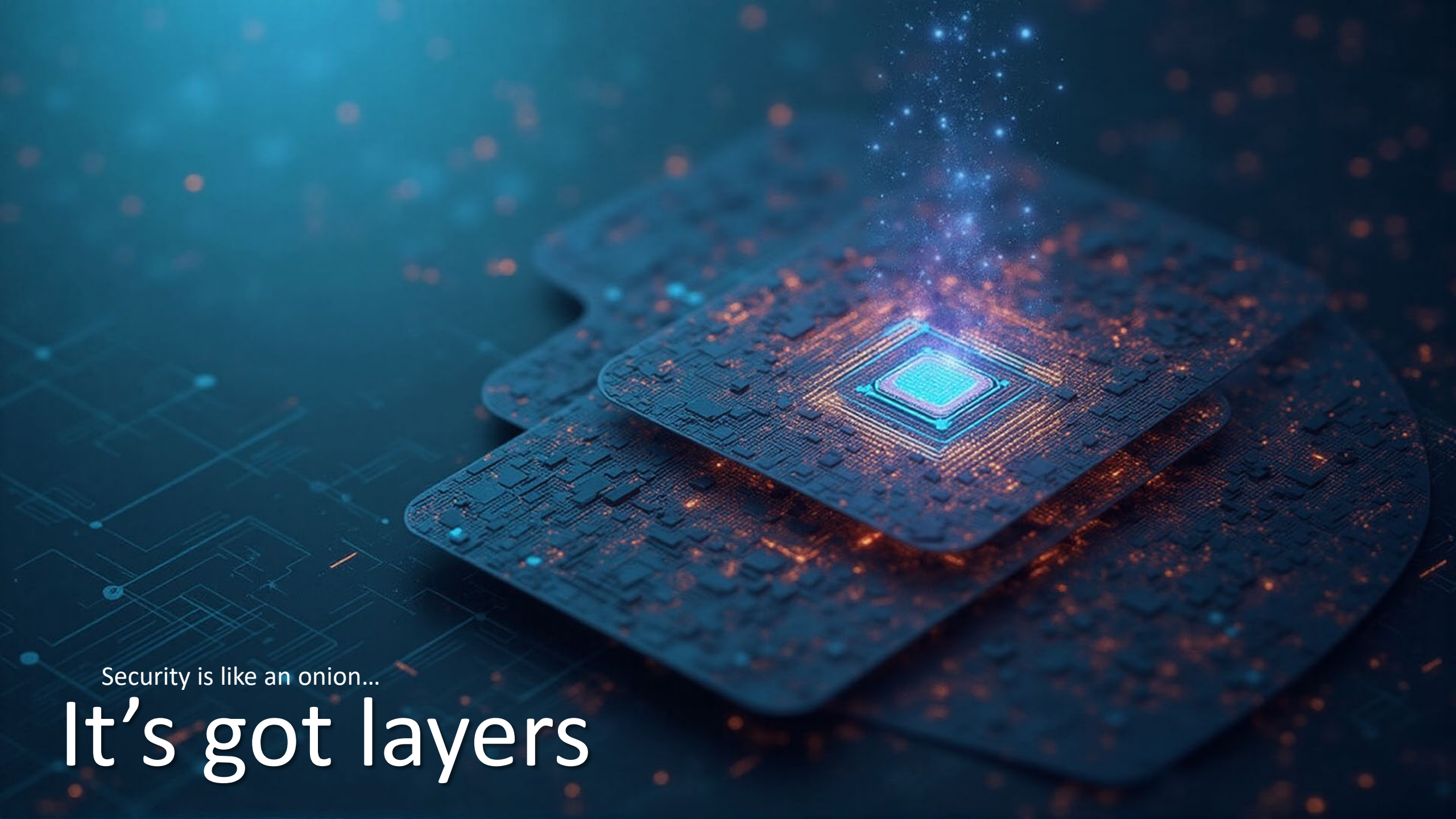

Ready?
42%
GO.

Cybersecurity Hygiene


BEFORE
WE START

We start with

Varied backgrounds…



Security is like an onion…

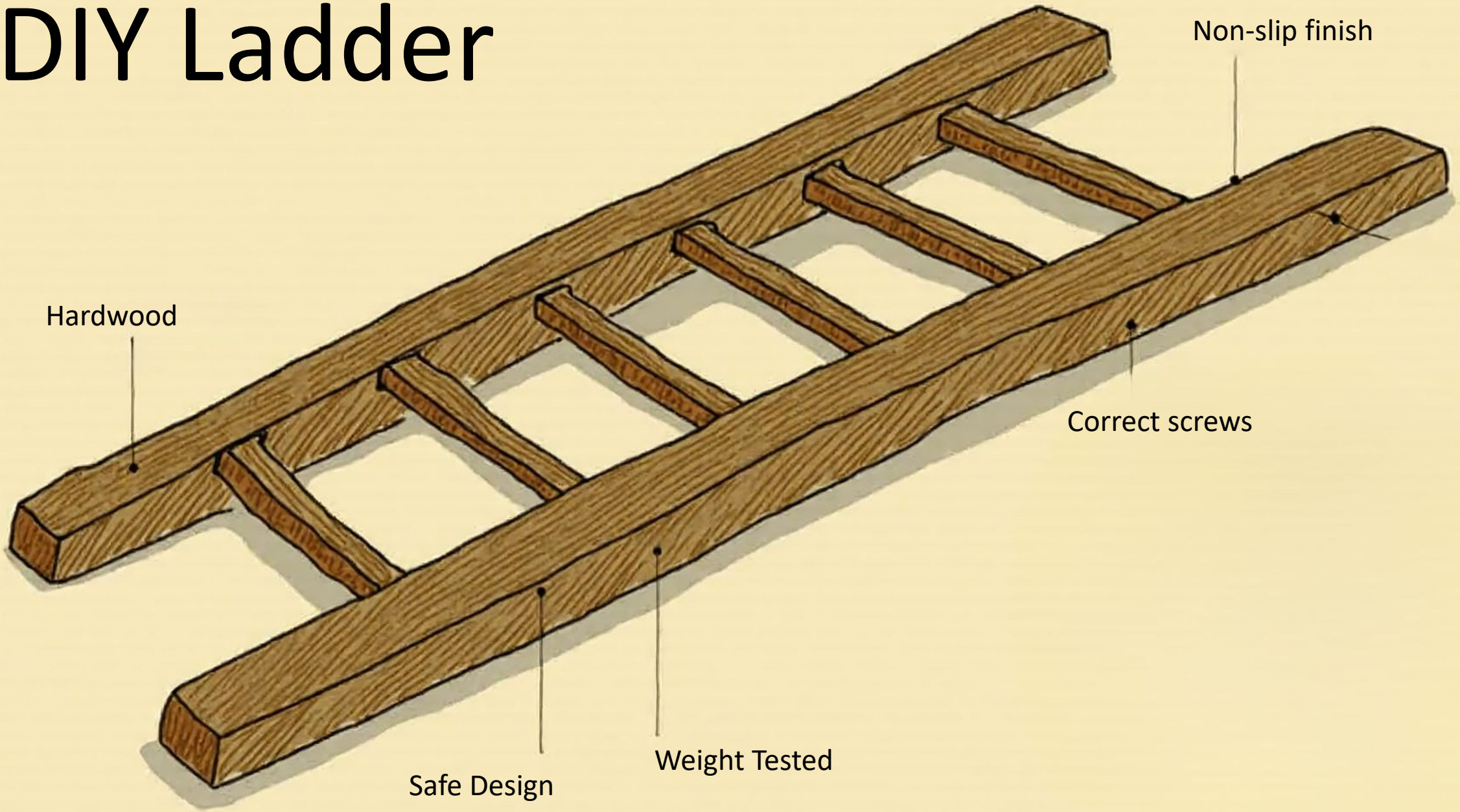
It’s got layers

consider

Trust

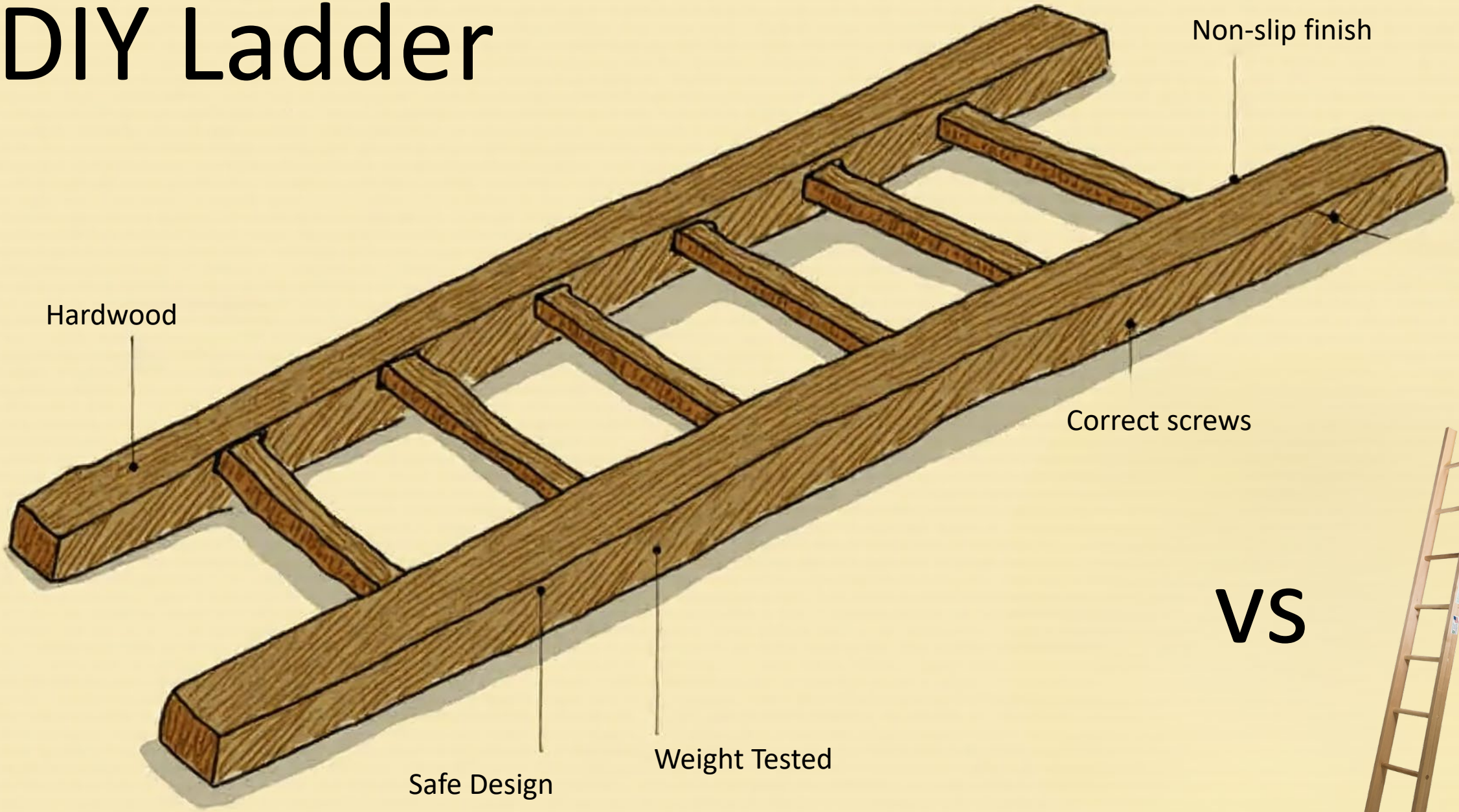
example

DIY Ladder



example

DIY Ladder



VS

Always follow institutional policies & procedures

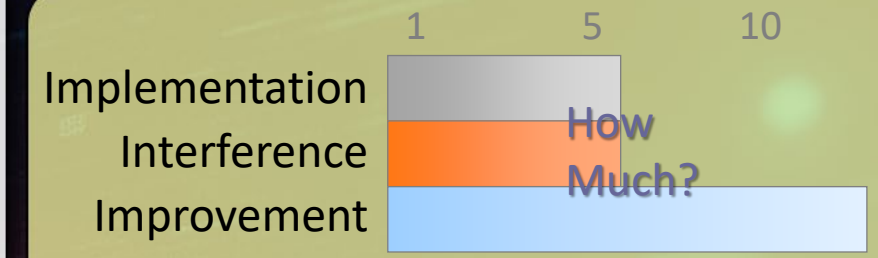
because it is better;

and for compliance reasons…

How Proactive Items Slides Work

Short Desc.

Tools, Tactics, and Techniqes



Bonus Tip(s)

How Reactive Item Slides Work

What just happened?

Geek-o-meter

How technical do I need to be?

What should I do about it?

Resources (for later…)

- UBC: https://privacymatters.ubc.ca/
- ARC: https://arc.ubc.ca/security-privacy/
- CCCS: https://www.cyber.gc.ca/en
- NSA: https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF
- KeePass Password Safe: https://keepass.info/download.html
- Bitwarden Password Vault: https://bitwarden.com/
- Cryptomator: https://cryptomator.org/
- Have I been pwned: https://haveibeenpwned.com/
- Security Now! Podcast: https://twit.tv/shows/security-now
- Interpol: https://www.nomoreransom.org/
- Browser Add-ins:
  - uBlock Origin Chromium: https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm
  - uBlock Origin Firefox: https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/
  - Privacy Badger: https://www.eff.org/privacybadger


GO
GO
GO

Something went wrong!

Any time something goes wrong or

Something doesn't look right or

I worry I've been hacked or

I think I just goofed up or

I just received a disturbing message.

Geek-o-meter

Stop Assess Plan Proceed (SAPP)
- A First Responder Technique:

STOP: Take a deep breath, don't do anything just yet, catch your breath, let the shock dissipate.

ASSESS: Take stock of the situation, observe, consider the current status. Collect the facts.

PLAN: Use the information you just collected to plan appropriate safe actions.

PROCEED: Only now should you start doing anything. Follow your plan (re-SAPP if needed).

This process should take seconds - minutes.

Unique Passwords (Secrets)

The single most important good habit:
Prevent one breach from impacting all your accounts.

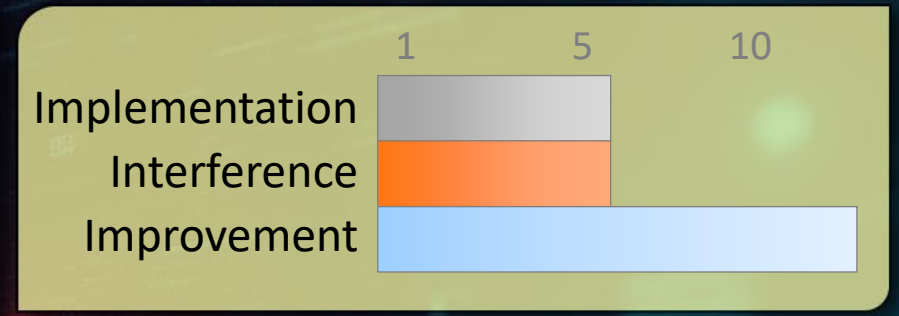
Remember how to build passwords or generate them rather than trying to memorize passwords

Size matters – use passphrases – not guessable

Use Passkeys (unique by design)

Your ssh or other key-pair should also be unique.

Only change them when necessary



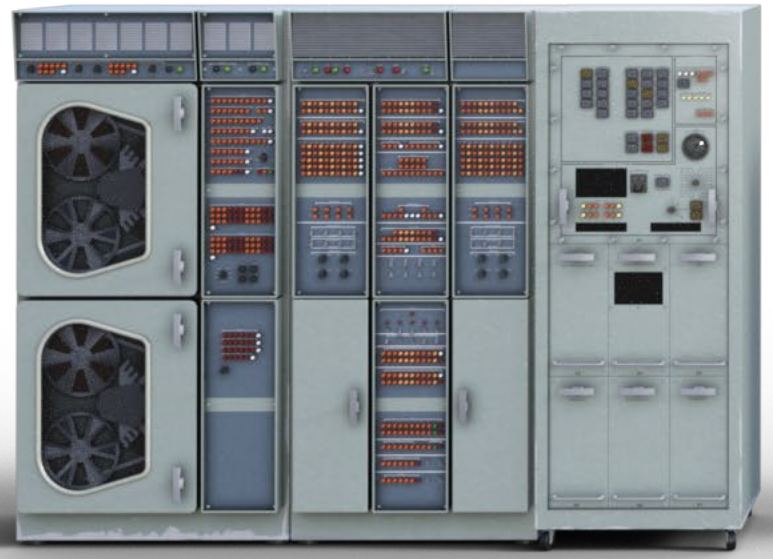
Bonus Tip:
Consider how hard it will be to type in on your mobile: minimize keyboard switching.

What's the

Big Deal?

Service A

Breached – your credentials stolen
Forced Password Reset
Notifications Sent



What's the

Big Deal?

Service A

Breached – your credentials stolen
Forced Password Reset
Notifications Sent

Stolen Credentials
Posted/sold

What's the

Big Deal?

Service A

Breached – your credentials stolen
Forced Password Reset
Notifications Sent

Stolen Credentials
Scripted Attempts
(within hours)

Service B (C,D,E,F….)

Has not been breached
No reset
No notification

https://haveibeenpwned.com/

Most people have at least one email listed at least once
…or will eventually.

The email address I have had since 1994 is listed in > 18

Depending on the breach, different information is included.

Unique Passwords (Secrets)

The single most important good habit:
Prevent one breach from impacting all your accounts.

Remember how to build passwords or generate them rather than trying to memorize passwords

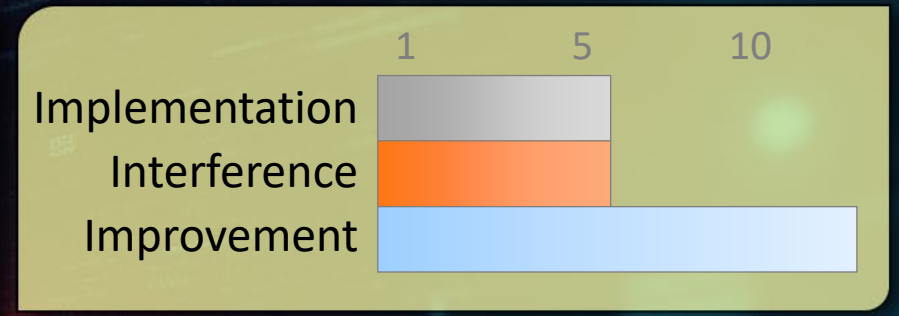
Size matters – use passphrases – not guessable

Use Passkeys (unique by design)

Your ssh or other key-pair should also be unique.

Only change them when necessary

NEVER share your password with ANYONE – ever.



Bonus Tip:
Consider how hard it will be to type in on your mobile: minimize keyboard switching.

Use a Password Vault

Single encrypted location to store and manage secrets.

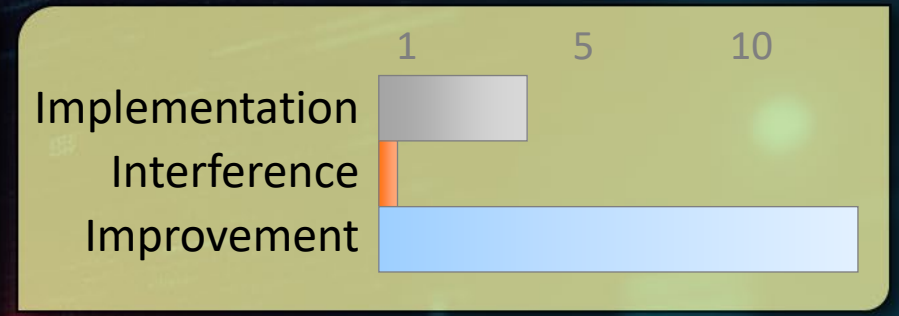
Generate your passwords for you

Store other kinds of secrets

Securely send information to others

Is actually faster... really!

Put the master password in your will.



Bonus Tip:
Keep it separate from the browser for extra protection

Use Multi-Factor Authentication

Passwords are a single point of failure.
MFA provides dramatically improved protection.

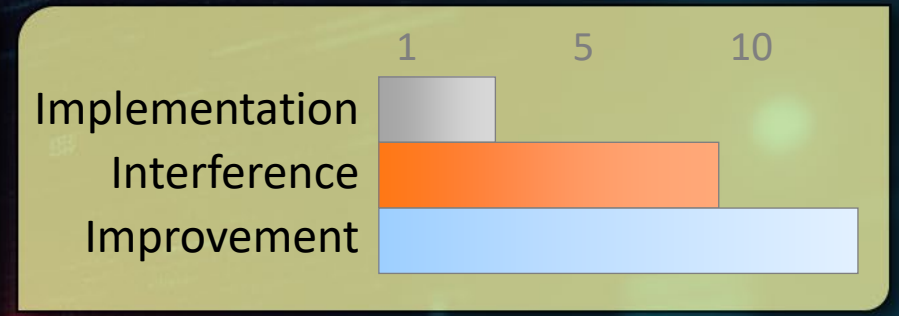
Something you have (token), or know (password), or are (your fingerprint)

SMS is insecure sadly, but still better than nothing

Many options exist, many systems support MFA.

EG: YubiKey, Google Authenticator, SecurID, etc…

Beware MFA – Fatigue (see slide on the topic)



Bonus Tip:
Ideally, have more than one MFA device registered (in case of loss!)

MFA Fatigue

I’m receiving constant “push” notifications from my MFA service (Microsoft or Duo etc…) But I’m not trying to login right now.

Geek-o-meter

DO NOT ACCEPT the MFA push.

This is likely a bot or criminal who may already have your username/email and password and is attempting to gain access to a MFA protected service.

If possible – MANUALLY navigate to the system in question. Login and ideally use a different MFA device to do so (so you can tell the difference between the criminal’s attempt and your own) then change your password.

If in doubt – contact the support/security department for this notify them and have them assist.

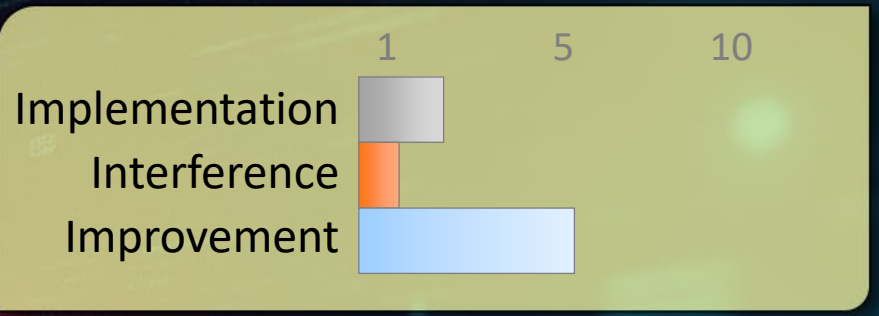
Protect Other Authentication Methods

Many services provide access with other (sometimes minimal) information.

Safeguard ALL information that can be used to authenticate you.

Eg: Your flight can be changed/canceled with nothing more than the booking number and your last name!

Don't discard/snapshot, and/or share anything with this type of information.



Bonus Tip:
As soon as your name is on something – treat it as sensitive, even when all the rest is mundane.

Protect any Recovery/Reset Pathways

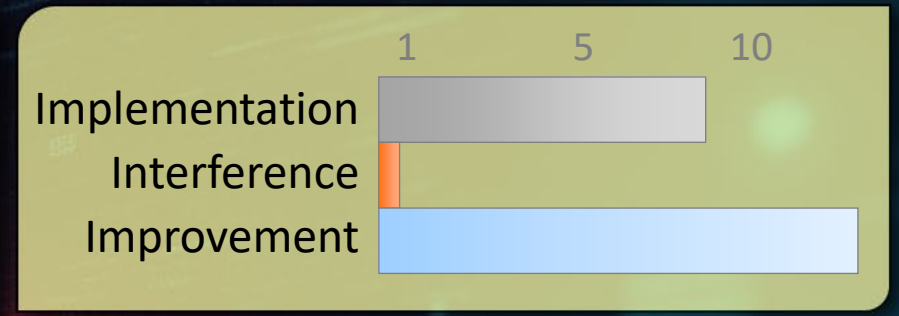
Password reset/recovery can bypass all other security You put in place.

Keep access to your recovery information secure. Especially if access to a single email account might potentially allow password resets to all your other accounts.

Periodically audit your accounts and ensure the recovery information including email and phone numbers are accurate and current.

Keep recovery MFA keys safe and locked away.

Consider establishing different recovery information for different accounts.



Bonus Tip:
Use a special recovery email address/phone number if you can.

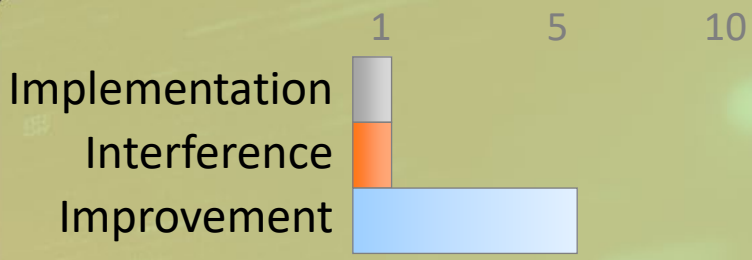
Think before you scan that QR code

QR codes can contain malicious links, trackers, and more.

Check for stickers over the real code or Whitespace on a poster.

View the link before you browse to it.

QR codes can contain more than just URLs eg: automatic WiFi connection information.



Bonus Tip:
If you generate QR codes – check to ensure the generator didn't alter the URL.

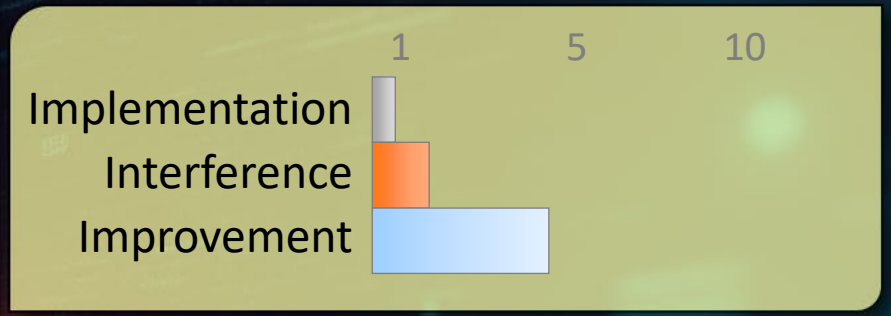
Avoid sharing your screen

Screen sharing can lead to accidental disclosure.

Instead, share individual applications.

Keep in mind that sharing a web browser window shows your bookmarks toolbar and ALL the open tabs.

Open a separate browser with only the tabs you intend to share in that window.



Bonus Tip:
Close as many applications as possible before sharing, your presentation will run faster too.

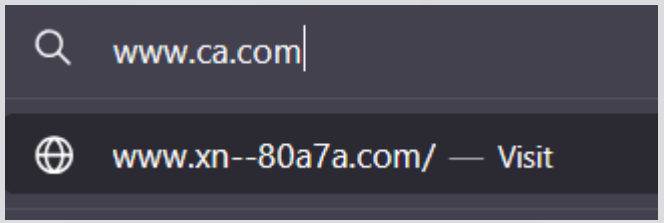
Bookmark ~~Important~~ Most Sites

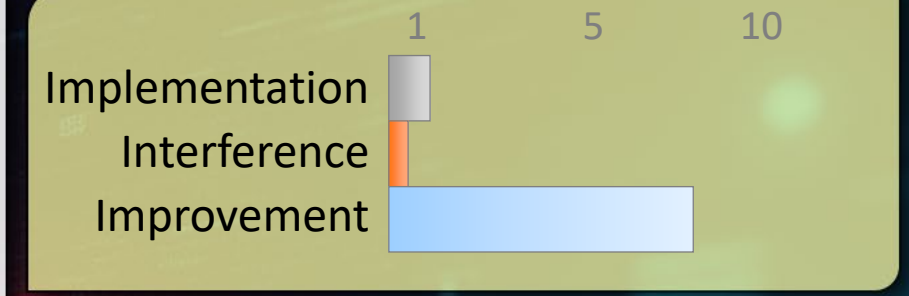
Ensures you do not typo/search the address and end up on a fake look-a-like fraud site

The saves you time while also making you more secure.

Cybercriminals frequently puschase domains that look very simiar or are common typos for real sites (eg: gooogle.com or faacebook.com or www.ca.com) to trick you to “sign-in” to their fake site or to deliver malware when you visit.

Using a bookmark ensures you always go to the real site.





Bonus Tip:
Store site URLs in your password vault as well for safe automatic access.

I recived a link

I just received a text message/email/DM/Post with link I must click to get more information or because dire consequences will happen or…

because it sounds really interesting

Geek-o-meter

ALMOST NEVER CLICK A LINK from a message.

SAPP!

Were you expecting this?

Instead try going to the source (use your bookmark) and check there.

Use another means to confirm the urgency (if applicable) or with the individual. Yes it takes time but is so much safer.

When should I click? In the rare circumstance that I was expecting it – had just initiated it request.

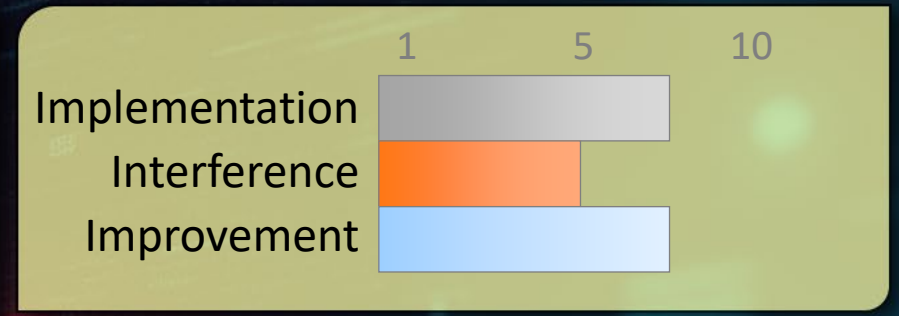
Travel: More than a blank phone

Just bringing a blank (burner) phone may not be enough
Also consider a letter explaining why!

Travel to some jurisdictions in the current geo-political environment can be… uncertain.

Wiping your electronic devices before travel is a good idea but this too may raise questions

Consider requesting a letter from your employer stipulating the requirement to travel with blank devices or have an explination ready to avoid complications.



Bonus Tip:
Search for yourself online – what would a border guard see?

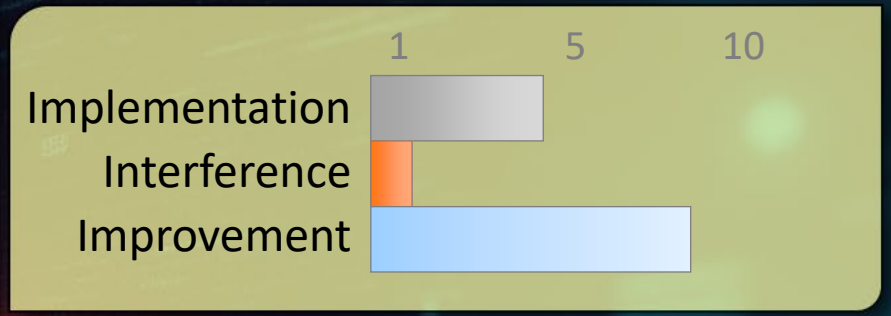
Audit Shared Folders

Ensure only the people required have access
Reduce disclosure risk and potential attack surface

Review what folders you share and who they are shared to (may need to use the web interface)

Do these people still need access? Do you still need the document in the cloud?

Revoke access and remove any documents that are no longer required.



Bonus Tip:
Knowing where your sensitive data is, makes this step easier.

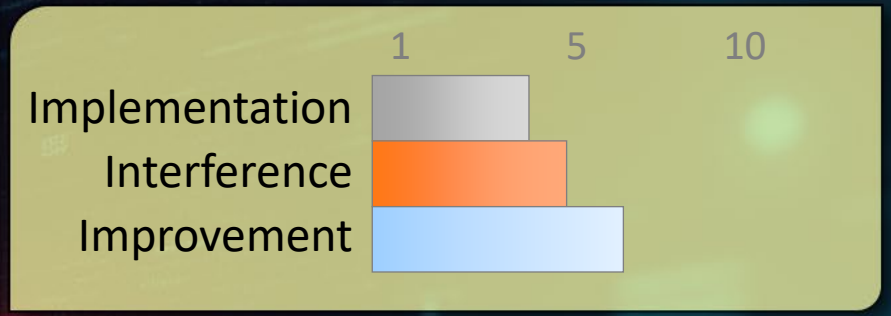
Photo Sharing – Hidden Data

Many cameras embed Lat/Lon and other information into digital photos.

Consider carefully what meta-data is included in photos you share.

Consider what is in the background of pictures (eg: sensitive information pinned to a wall) or in reflections.

Expect shared photos to be used by others (remember there is no such thing as private "sharing") Don't share what is too sensitive to share.



Bonus Tip:
Most operating systems allow easy removal of meta-data via a right click on the picture.

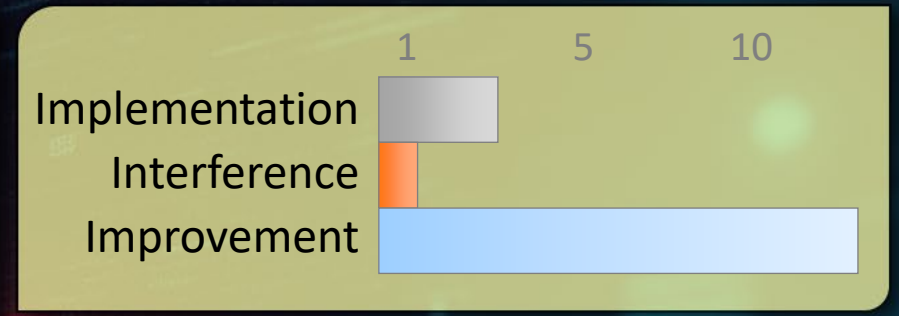
Delete Unnecessary Information

What isn't there, can't be stolen or mishandled.

Consider what data you have and why.

Just like shredding paper documents – 'securely' delete data that is no longer required in any particular location.

Yes, it's really just that simple.



Bonus Tip:
This can save space on your hard drive as well.

Apply Software Updates

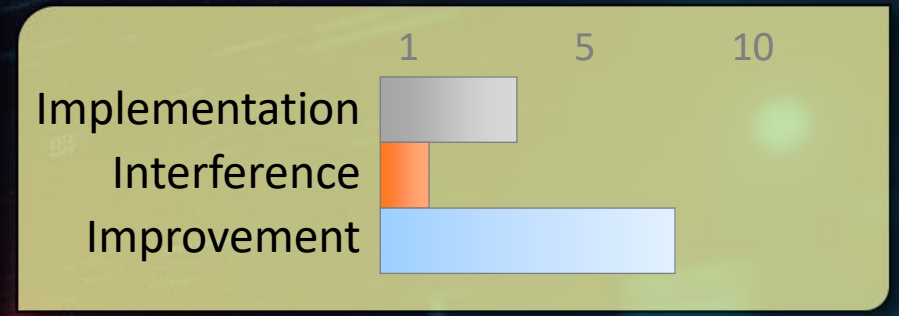
Smart people are working hard to fix vulnerabilities: Take advantage of that (usually free) protection.

Computers, phones, TVs cars, and now even toasters run on software/firmware. Keep that patched by applying reputable updates from known sources.

In some respects, the closer the device is to the outside, the more critical it is to patch.

Do not only assume automatic updates (confirm)

Reboot! (Weekly at a minimum) – including your phone.



Bonus Tip:
Set a reminder to check for patches to less front-and-centre equipment like your router.

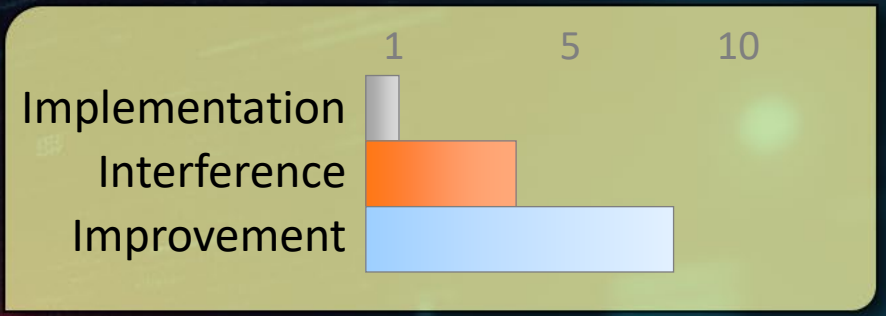
Don’t Blindly Copy and Paste Code

It’s easy to hide content on the web through CSS or JS.

Malicious code can be hidden in a multitude of ways on web sites.

Hidden code in snippets may or may not originate with the content publisher.

In all cases pasting into a “dumb” editor first will help confirm what is actually being pasted before it goes into the shell or application.



Bonus Tip:
Set your terminal to warn about multi-line paste.

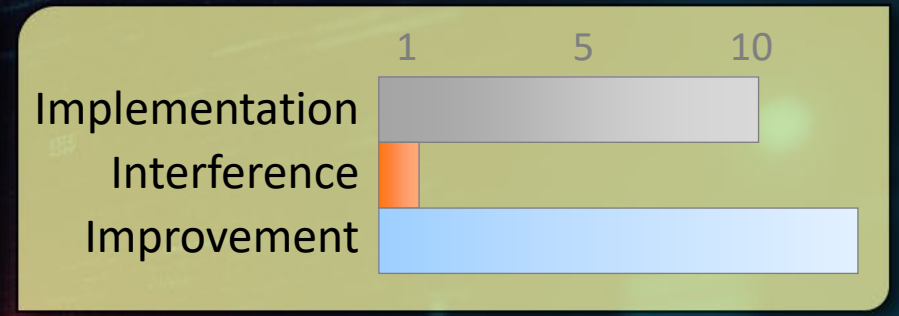
Advanced Tactic

Replace Old Appliances

End of life connected appliances are insecure.

When connected “smart” devices are no longer receiving patches from the vendor, the only safe solution is to disconnect them from the network (the whole network) or purchase a replacement.

These devices are no different than your computer – they have just as many vulnerabilities (or more) and require patching. If they exist on your network they can be used to damage any/all your other devices or those of others.



Bonus Tip:
Start saving early for replacements – lifespans are typically 5-10 years depending on the device.

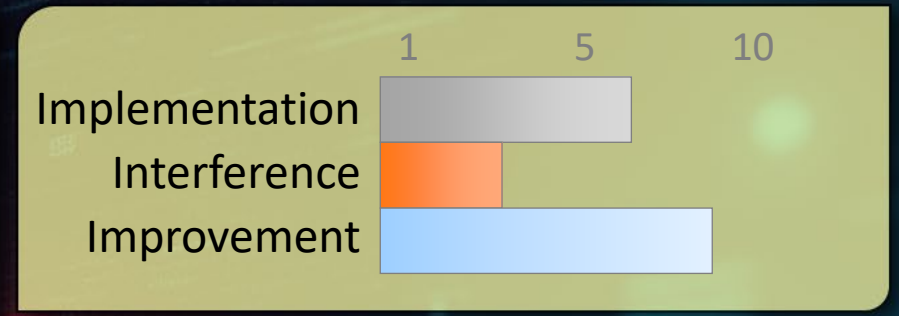
Audit Authorized Apps

Ensures only currently trusted apps have access and reduces your potential attack surface

Visit each social web site. Typically under account settings or privacy there is a section for applications.

Do you know each app listed? Do you still use it? Is it worth risking the level of access it requests for the benefit it brings?

Revoke access to any apps you don't need or trust.



Bonus Tip:
You can always authorize the app again later.

Supply Chain Trust

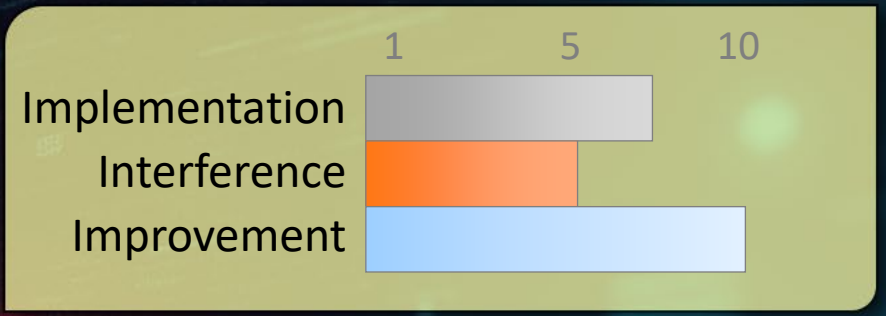
We must know what is in the software, to trust it.

As code becomes more modular and sourced from a larger number of different locations, the ability to trust that code is “safe” becomes significantly more challenging.

Use the minimal set of libraries, frameworks, and dependencies. Beware AI “Slop-Squatting”

Sometimes custom written code is actually faster and more efficient.

Check/Maintain a Software Bill of Materials (SBoM)



Bonus Tip:
Diff library updates to review changes.

Implement scanners for known injections.

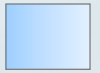
Advanced Tactic

AI Deep-Fake Plea for Help

I just received a voice message/call from my child/spouse/relation in their voice with an urgent need for help.

They desperately need me to send money/gift cards/my bank account etc…

Geek-o-meter



Faking someone's voice is VERY easy.

SAPP!

Contact them back to verify. Double-check with their partner, use another means (text, email, Slack, Discord, etc… preferably something not using their phone)

Use other channels to confirm their location.

Be proactive pick a code-phrase or ask a question only they could possibly know the answer to. EG: When was the last time you fed your cat Spot? (knowing full well there is no cat Spot!)

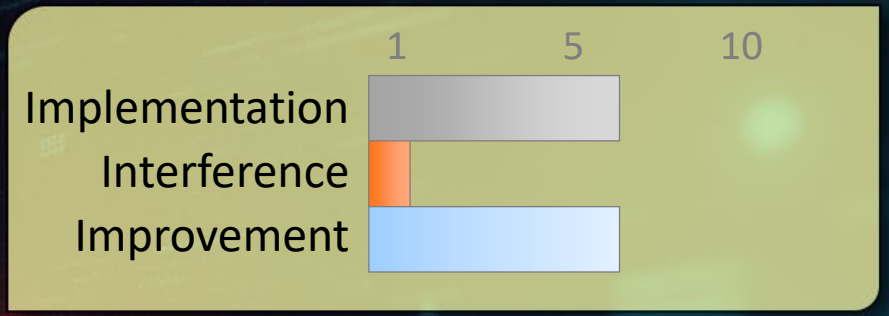
Securely Delete/Encrypt Files (Cloud)

Deleting a file from the cloud is similar to your HD, except on the cloud you have no way to ensure deletion.

There is no clear way to ensure a file deleted from “someone else’s computer” (aka ‘the cloud’) is actually deleted or just hidden.

In essence you must trust the cloud provider to ensure deletion has occured.

The only way to protect sensitive information being entrusted to someone else is to encrypt it before it is placed in the cloud in the first place.



Bonus Tip:
See the could data encryption slide for a possible mitigation for this issue.

Multiple Browsers

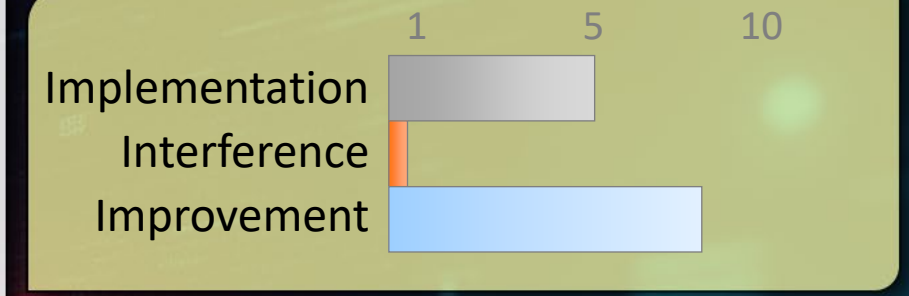
Use different browsers for different purposes.

Reduces Tracking

Reduces the risk of the “wrong account”

Allows for reduced extensions in the browser used for higher risk activities.

Re: Bonus Tip:
see: https://addons.mozilla.org/en-US/firefox/addon/multi-account-containers/



Bonus Tip:
Firefox Multiaccount-Containers add-on can also help with account segregation.

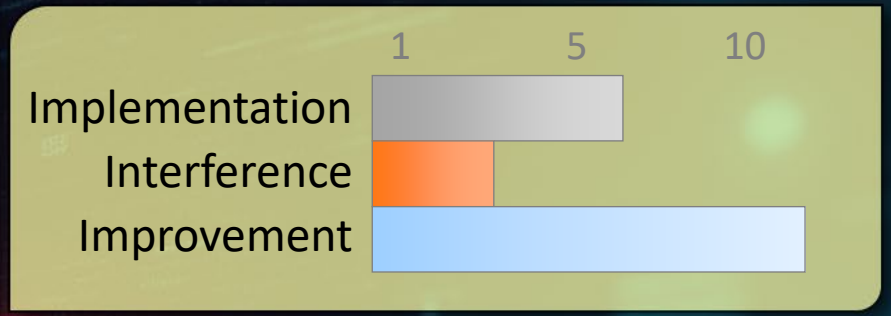
Use Encryption (cloud/file/database)

Encrypting data adds protection both in transit and at rest, usually adding an additional layer of security.

One of the simplest ways to encrypt any document is to use ZIP with a strong password. This comes pre-installed for most operating systems.

There are many other (better) options for encryption that automate the process but require special software:

https://cryptomator.org/



Bonus Tip:
If using password ZIP encryption – keeping the password secure becomes critical.

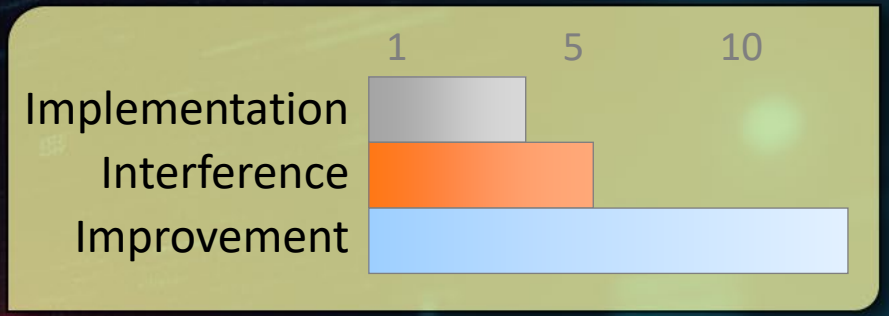
Security Questions & Answers

Providing known/discoverable information is insecure
Limit social engineering and credential reset attacks.

Just because the form asks for your birth date, favorite pet, or mother's maiden name, does not mean that is the information you should enter: polyinstantiation.

Free form answers are preferable and can be used for additional passphrase-like responses.

Many third parties do not encrypt their security Q&A – providing the same answers in many locations becomes a significant risk.



Bonus Tip:
Store the responses in your password manager along with the password in the notes field.

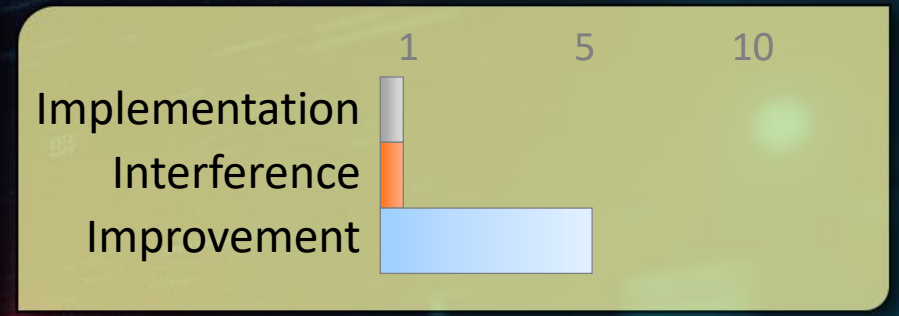
Show File Extensions

Icons and filenames can be misleading.

Windows hides file extensions by default but it is easy to make a file that does one thing – look like something else.

EG: document.pdf vs document.pdf.exe

If extensions are hidden you can't tell the latter is actually a program.



Bonus Tip:
Also turn on hidden files so you can see the entire picture.

Keep Work and Personal Identities Separate

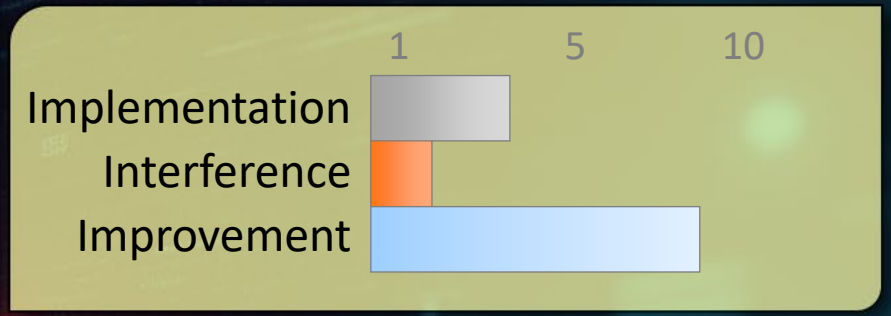
Your business contact information is public
Your personal contact information is private

It can be tempting to allow the lines between work and personal to blur (no need to check 2 emails etc.) but…

Your employer and other staff can potentially see all your business email.

If you work for a public institution – FOI requests could make the content of any work email and chats public.

Jobs change… your personal contact information shouldn't need to change because of that.



Bonus Tip:
Even at work consider if you want to give out your email (conference spam)

Broadcast Emails

Don’t send emails that look like phishing.

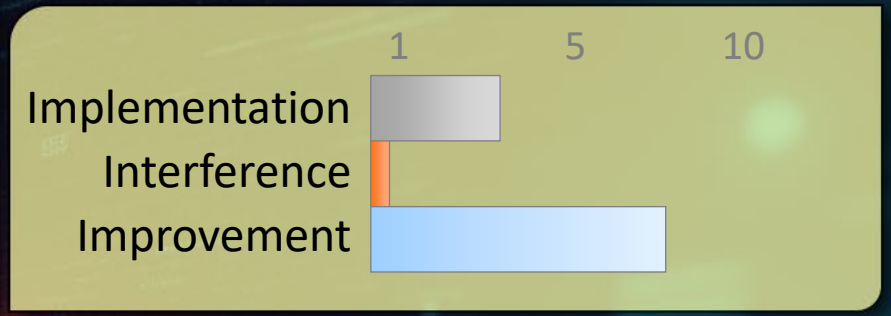
Support the training and awareness in your organization.

Avoid urgency language.

Use institutional email servers (no external services)

If you must include a link - send a timely warning first.

Don’t use tracking URLs if you have links.



Bonus Tip:
Do not include any links in broadcast email if you can avoid it. Never link to pages that require login.

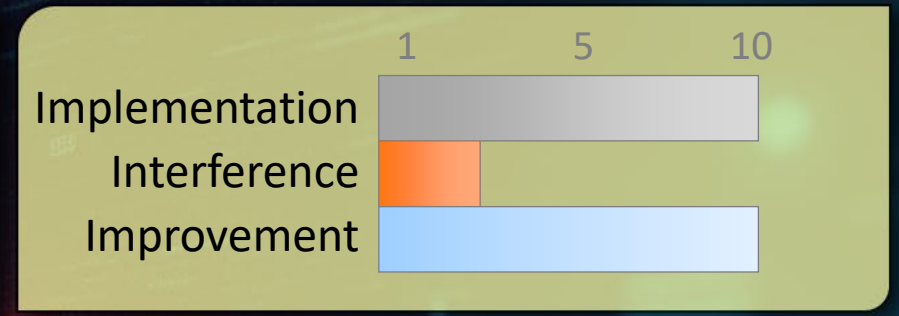
Use a VPN

All unencrypted traffic over a network segment is subject to sniffing
Prevent credential and data theft on un-trusted networks.
Prevent DNS cache poisoning attacks.

Basic: Subscribe to a trusted VPN service
Advanced: Set up your own VPN (openVPN)

http://www.pcmag.com/article2/0,2817,2403388,00.asp

Configure this for all mobile devices and use it any time you're on an un-trusted network.



Bonus Tip:
DNS lookup can sometimes be faster over a VPN.

eTransfer Autodeposit

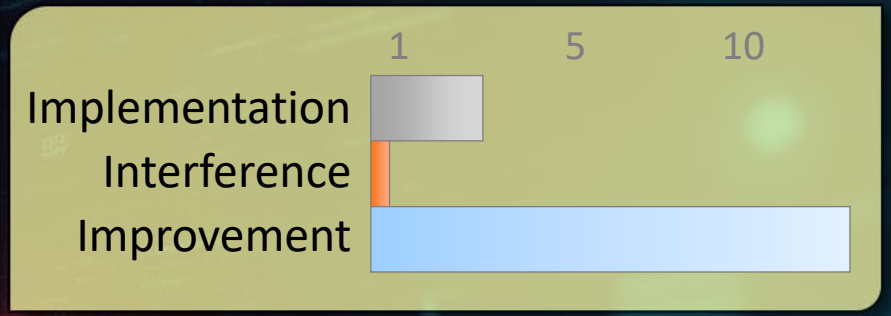
Register your email for autodeposit with eTransfers.

No need for passcodes that can be intercepted or guessed!

Easier to comply with bank terms of use
(no repeated passcodes)

Faster for everyone!

Reduces your liability.



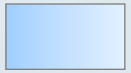
Bonus Tip:
Use a custom email address that is easy to remember

My Screen Froze

I just visited a web page and now there is a message with a phone number telling me to call Microsoft/<insert large company name here> Support to help unlock.

There may even be a recording or what looks like additional activity appearing on the screen.

Geek-o-meter



DO NOT CALL/Click/Text.

Companies like Mictosoft do not provide this type of support or monitoing – it's a scam trying to defraud you.

Try <alt>+<tab> to see if you can switch tasks, your screen may not even be frozen but showing an overlay that only makes it appear to be.

Reboot using the power switch (or physically unplug from the wall)

If the problem persists – disconnect the machine from the internet and seek technical support from the IT support you USUALLY use.

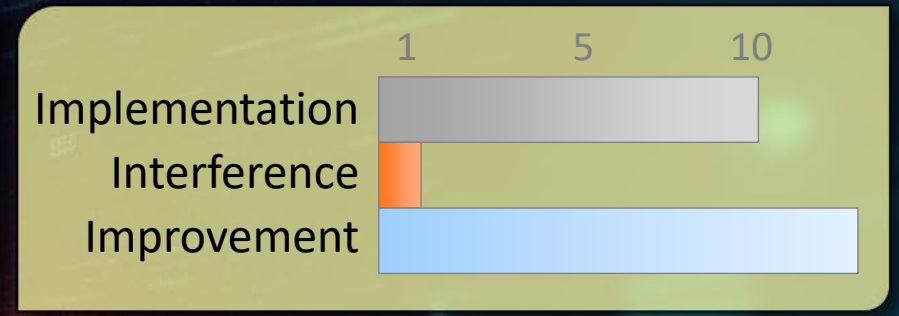
Have Backups and Plan to Restore

A backup that can't be easily restored is useless and might be the only option after a ransomware attack.

Avoid becoming too entangled in a proprietary system that only works after it's installed.

Remember to think about the security of your backup as well (eg: high-profile iCloud breaches)

A simple external hard drive caddy is reliable and cost effective (keep it disconnected except during backup)



Bonus Tip:
Test your restoration plan periodically – ensure it works.

Reset Default Passwords

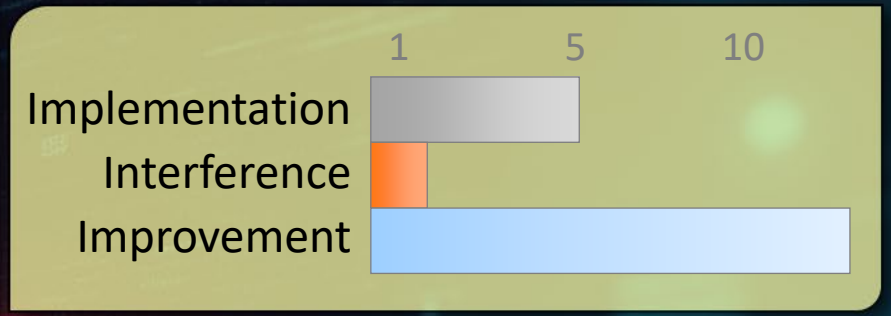
Mitigates bots / scripted compromise
Easier for you to access

Make it a habit to always change the default credentials first, as soon as a new device/software is turned on or any time it requires a factory reset.

This includes the router/modem provided by your ISP

Read the manual. Every device is different and will require a slightly different process.

When in doubt, use your Google-Fu!



Bonus Tip:
Reset the default usernames too if you can!

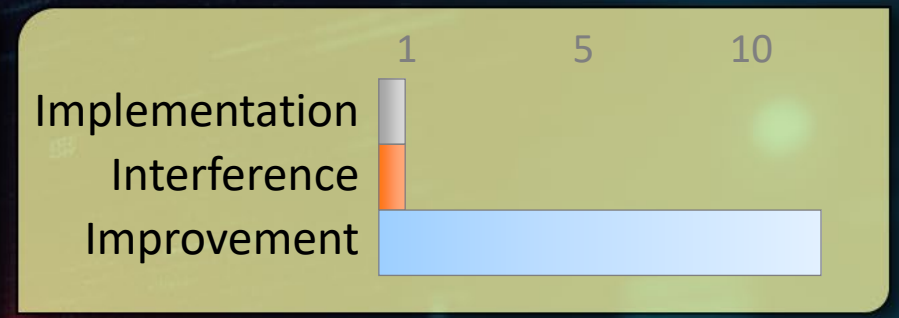
Social Sharing and Privacy

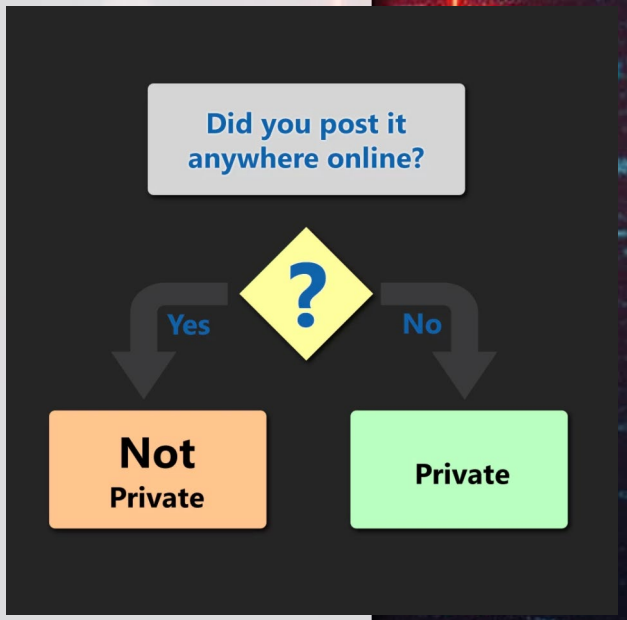
There is, arguably, no such thing as a setting to ensure “private” sharing.

Privately shared items can be re-shared, screen captured, copy and pasted, stolen, exposed, leaked, etc…

Always think first about what you are sharing because once posted, it’s impossible to un-share.

Think about who you are trusting.





Bonus Tip:
Set everything to “public” on social sites helps promote safe sharing behaviour.

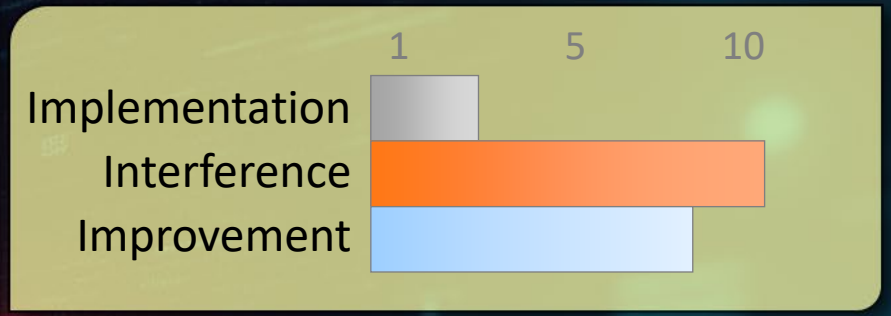
Sign-out

If someone gains access to your device… they have access to everything you're already signed into.

This also prevents information disclosure across different web sites and/or social media sites.

Signing out adds another layer of security.

Modern browsers sometimes allow different accounts or private browsing that further segment access across different apps.



Bonus Tip:
Wiping cookies will sign you out of most services in a single step.

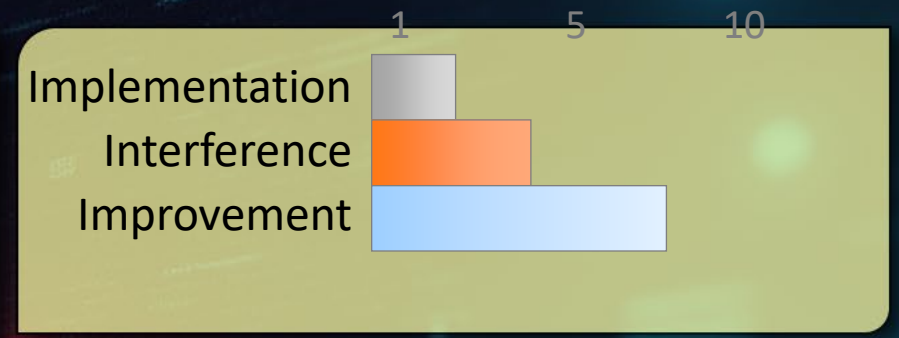
Block Ads, Trackers

Ads are riddled with security holes, frequently serve malware and you likely don't want them anyway.

Many browser plug-ins make this effortless and still give the option to allow Flash or ads when you need them (including by-site or by-page white-listing).

Trackers may facilitate information aggregation.

Can also speed up browsing and save data on mobile too.



Bonus Tip:
Blocking trackers may also help prevent against Identity theft.

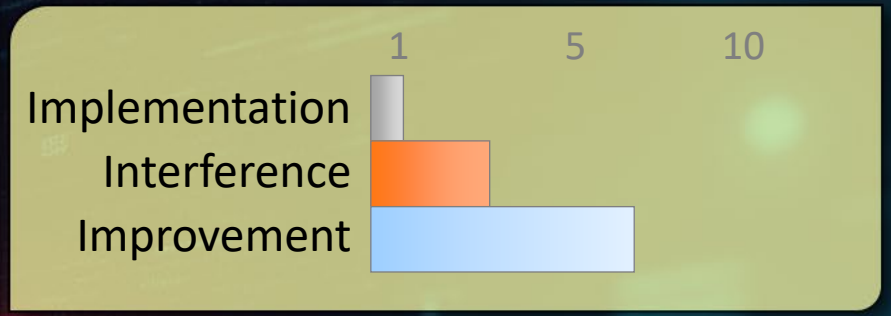
Browser Memorized Secrets

Allowing a browser to memorize your password, CC, etc Defeats security layers of protection.

Leverage a password vault instead that keeps your secrets safe and requires authentication to access.

Browsers may memorize old or incorrect information

Anyone with access to your system has access to what has been memorized.



Bonus Tip:
If you use a password vault, the memorization function does not save any time.

Authenticate to Unlock

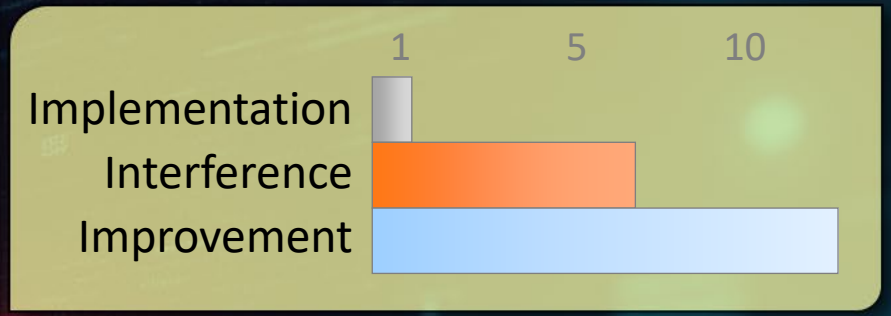
An unlocked device in the wrong hands has full access to everything you normally do.

A good and strong password is the most secure (most painful)

If choosing a pattern avoid starting at a corner and cross over the path at least once.

If using a PIN avoid “guessable” items (dates, phone numbers etc)

Keep your screen clean to avoid telltale fingerprints.



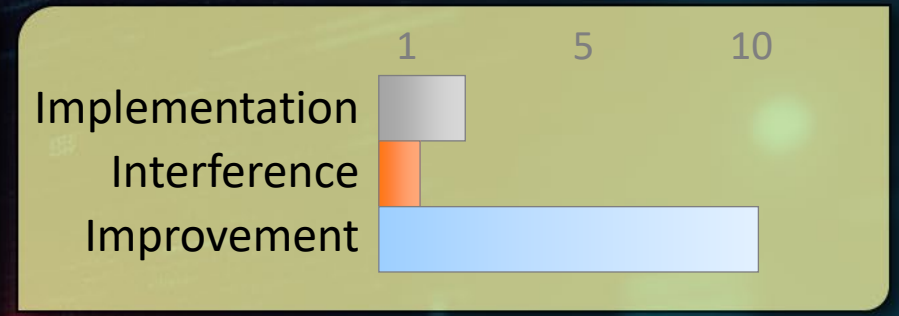
Bonus Tip:
Biometric unlocks may be fooled or broken entirely.

Shoulder Surfing

Protect sensitive information from strangers looking over your shoulder.

There is a reason the bank/credit card keypads remind you to protect your pin. It is very easy for other people to watch what you are doing and gain valuable information when you unlock devices, or enter passwords.

Also, always consider what information might be visible on your screen, especially in busy locations like an Airport or at a conference.



Bonus Tip:
Laptop screen privacy filters ($30) provide extra protection in busy locations

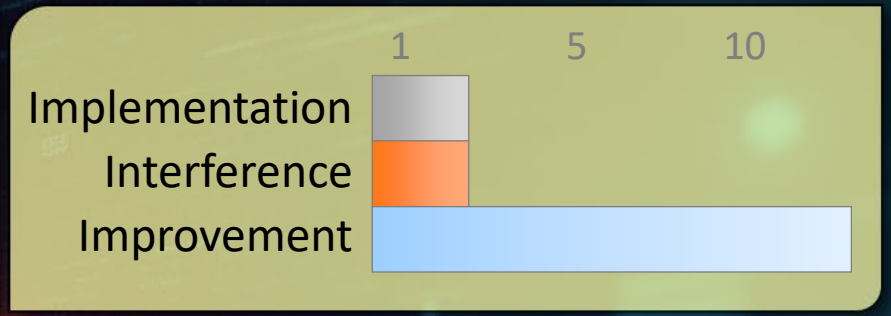
Power Off

IOT (and other) devices can't be used, or compromised, while they are without power.

Use a power bar and physically disconnect them from power (many devices are still in 'standby' when the power is connected and the main power switch is off)

If the device needs to stay on so the device doesn't reset, and it has a wired connection, consider powering off the network switch or access point that connects it to the network instead.

Do you really need your Fridge online? Avoid connecting devices to WiFi in the first place as another option.



Bonus Tip:
This will also save you money in electricity charges.

Be wary of USB devices

USB keys are risky for malware and information loss
USB ports provide hardware level access to systems.

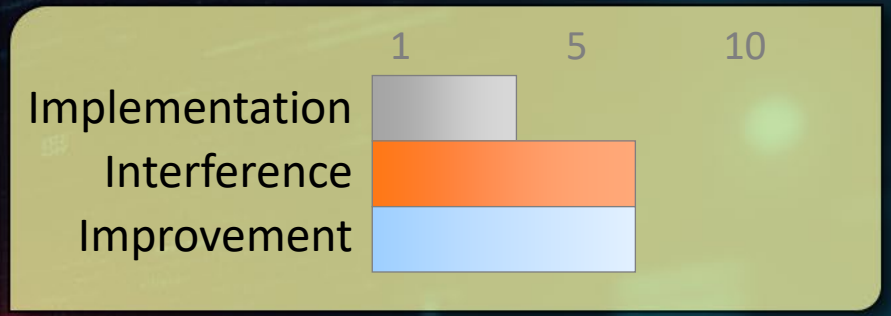
Turn off auto-everything for USB devices and learn how to prevent auto-launching if your OS supports it.

Do not use “found” or “free” USB keys unless you have reason to trust them.

Do not loan USB keys.

Encrypt any sensitive data stored on a USB key.

Think about where you are charging your mobile devices (get a USB condom https://shop.syncstop.com/collections/buy)



Bonus Tip:
Circle-check your desktop periodically to look for unknown dongles.

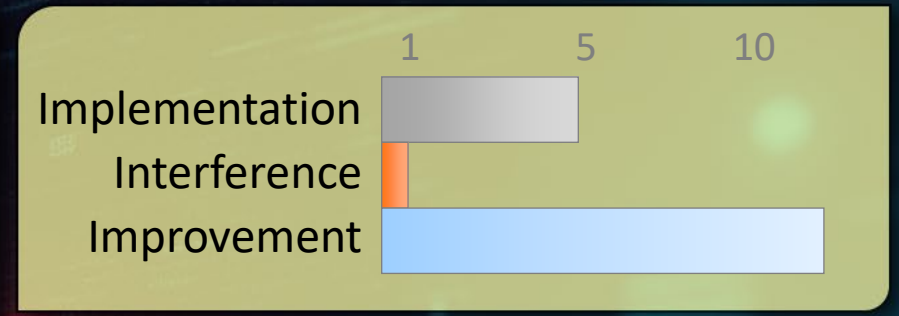
Identity Theft

Be aware of what you share across all sites, rather than just what is shared on a single one.

When considering what you share online, look at the aggregate data across all sites and not just one at a time.

Search for Yourself (don't stop at the first page)

Imagine what someone in possession of all that information might be able to convince a customer service representative… Could they pretend to be you with a convincing sob-story? (this happens all the time)



Bonus Tip:
Lie!

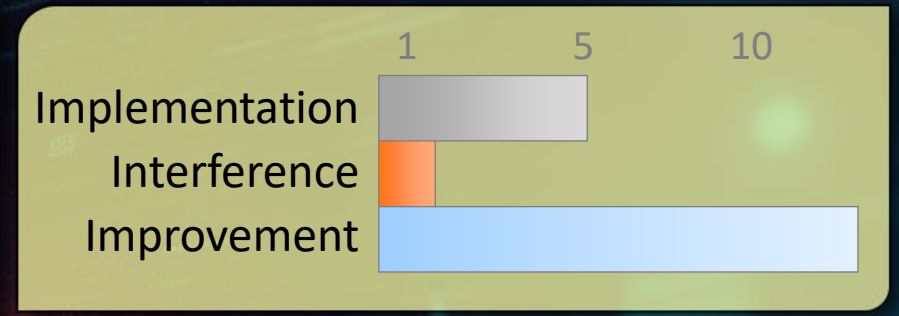
Use a fake birth-date (same year) on sites for age validation.

Cameras/Microphones can Record

Many compromises allow the camera/microphone on a device to record – keep that in mind.

Cover the laptop camera (and microphone) This is not a myth.

Consider where else you have devices that could be watching or recording you, Smart TVs, Baby Monitors, DropCams, your phone etc.



Bonus Tip:
Sometimes there isn't much you can do apart from being aware.

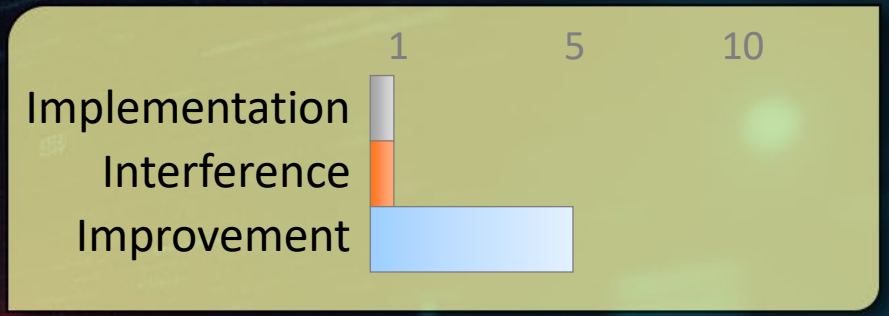
Be wary of USB charging stations

USB ports provide hardware level access to systems.

Think about where you are charging your mobile devices. It may be more than just power.

Use the AC wall power and your own adapter/power-bank instead of any provided USB ports.

Bring your own cable (power only) or get a USB condom
https://shop.syncstop.com/collections/buy



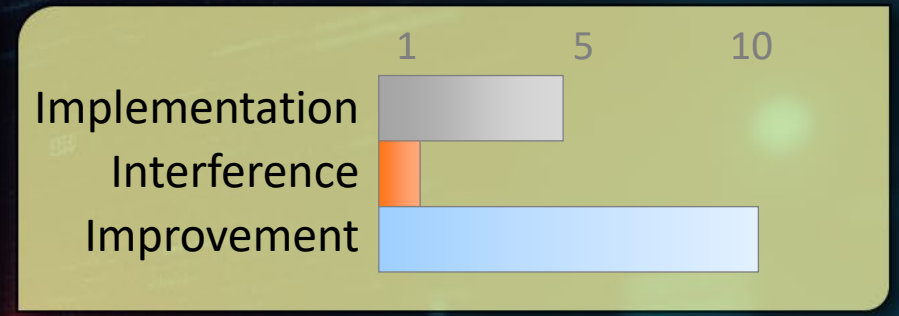
Bonus Tip:
Cars with USB ports can capture a lot of your personal information if you connect – read the privacy policy!

Encryption at Rest

Encryption protects confidentiality on multiple levels, the more mobile a device, the more it matters.

Most modern systems include the ability to turn on encryption. This includes desktop and laptop disk drives, mobile phones, even some USB keys.

In general encryption should always be enabled, but the more likely a device is to be lost or stolen the more important it becomes to encrypt.



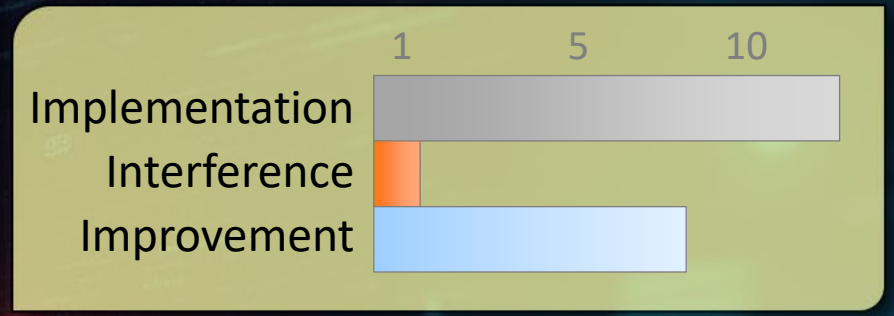
Bonus Tip:
The encryption key (or recovery code when applicable) must be very carefully secured. Use a Password Vault.

Segment your IOT devices

A more restricted network segment helps protect You from your own devices should they be compromised.

Create a separate network (buy an additional WiFi router) just for your IOT devices. Assign a completely different subnet address range (and perhaps class) to this network.

This network can be much more restricted and inbound connections limited even more than perhaps would be feasible on your main network.



Bonus Tip:
Restrict even connections from your primary network to/from the IOT network.

Advanced Tactic

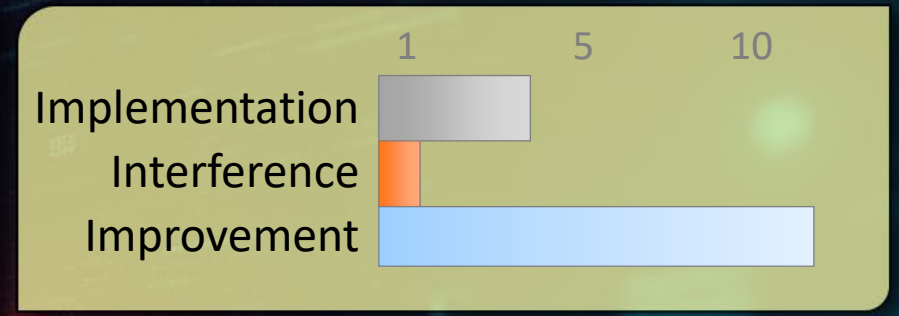
Sanitize before Disposal

Deleting a file from a storage device usually isn't enough to ensure it can't be recovered.

After deletion you need to either ensure all storage is re-written (this typically requires multiple passes) Several free software applications exist to help with this process.

or

Physically destroy the storage, rendering it unreadable.



Bonus Tip:
A factory reset does NOT erase mobile devices.

Advanced Tactic

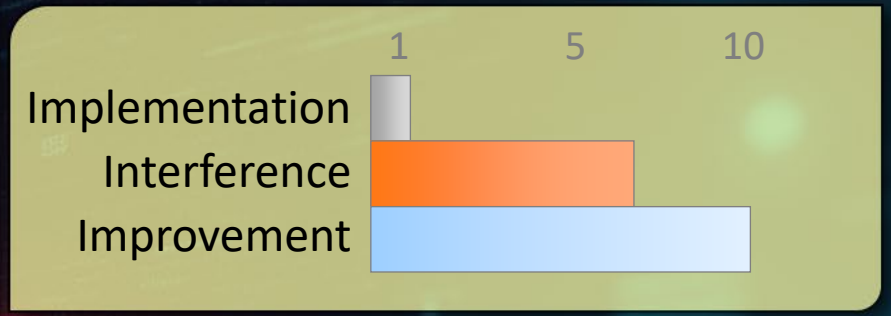
Enable Quick Auto-Lock

An unlocked device in the wrong hands has full access to everything you normally do.

Set your phone, tablet, and laptop to auto-lock after a short duration (no more than a few minutes).

Consider changing the duration based on current risks (eg: at home vs at a conference)

Get in the habit of manually locking your devices (this usually saves battery too).



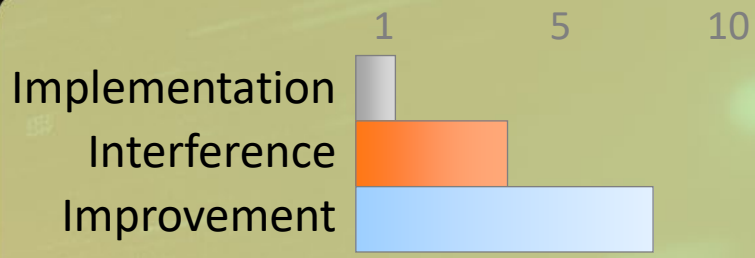
Bonus Tip:
Display lost and found information on your lock screen!

Avoid Lock-Screen Disclosure

Information displayed on a locked phone can be highly sensitive and bypasses security controls.

Ensure phone settings prevent the display of content like text messages, email, notifications directly on the locked phone.

Many services use a SMS code to reset a password, this shouldn't be displayed on a locked phone screen – the implications of this can be more far-reaching than expected.



Bonus Tip:
Display only the minimal lost and found information on your lock screen!

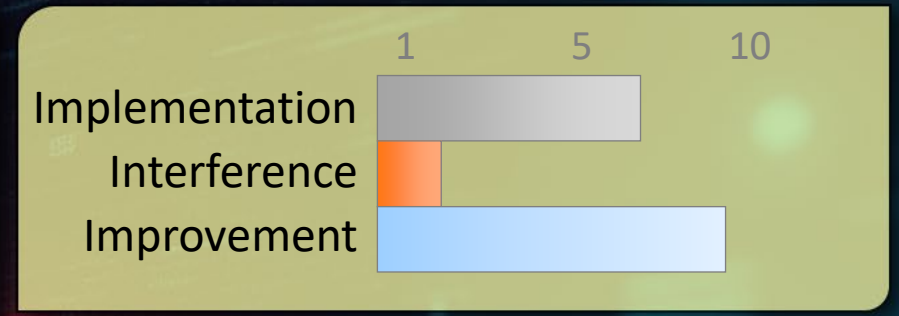
Guest infection through WiFi

Even a trusted friend may have an infected system, Sharing your WiFi could infect your entire network.

Create a separate network (buy an additional WiFi router) just for your guests. This also means you don't share your primary password and change the guest one periodically.

This keeps guests from accessing anything on your network that may not be properly secured (accidentally of course)

Combine this with the "guest access" on your primary wifi network for trusted access when required (see the bonus tip)



Bonus Tip:
Some routers offer a "guest network" that is just a different password on the same network.

Let’s keep in touch

email: scott.baker@ubc.ca

blog: https://scottbaker.ca/

LinkedIn: https://www.linkedin.com/in/pawprint/