

Introduction

This page intentionally not left blank.

Scott Baker

Drinking from the firehose





Before the deep-dive...
Why are we really here?

A simple goal...

Facilitate Research.





YOU'LL
NEVER
CLOSE
YOUR
EYES
AGAIN

INVASION OF THE DATA SNATCHERS

A ROBERT H. SOLO PRODUCTION OF A PHILIP KAUFMAN FILM "INVASION OF THE BODY SNATCHERS" DONALD SUTHERLAND • BROOKE ADAMS • LEONARD NIMOY
JEFF GOLDBLUM • VERONICA CARTWRIGHT SCREENPLAY BY W.D. RICHTER BASED ON THE NOVEL "THE BODY SNATCHERS" BY JACK FINNEY PRODUCED BY ROBERT H. SOLO DIRECTED BY PHILIP KAUFMAN

NEVER FORGIVE DESIGN



But,
does research data
really need

Security?

It's all going to be published anyway
right...

...right?

So, do all research projects really need security?

YES!



Security

Nine Iranians accused of cyber-swiping 30TB+ of blueprints from unis, biz on Tehran's orders

Gang pilfered files from 320 colleges, 47 companies in 22 nations, Uncle Sam claims

By Thomas Claburn in San Francisco 23 Mar 2018 at 20:36 20 SHARE



The US Department of Justice and Department of the Treasury on Friday **charged nine Iranians** with carrying out a series of internet attacks on more than 300 universities and 47 companies in the US and abroad, as well as federal and state agencies and the United Nations.

“Spear phishing messages, according to the indictment, would appear to be from another professor inquiring about one of the target's articles and would include a link. Clicking on the link would take the victim to a confusingly similar domain to the victim's university and present a fake login page.”

“They would collect names and email addresses for employees and then try lists of commonly used passwords. The indictment does not reveal how many accounts were compromised in this way.”

“With credentials stolen in this manner, the attackers were able to exfiltrate 31.5 terabytes of academic data and intellectual property.”

Just one recent
Example

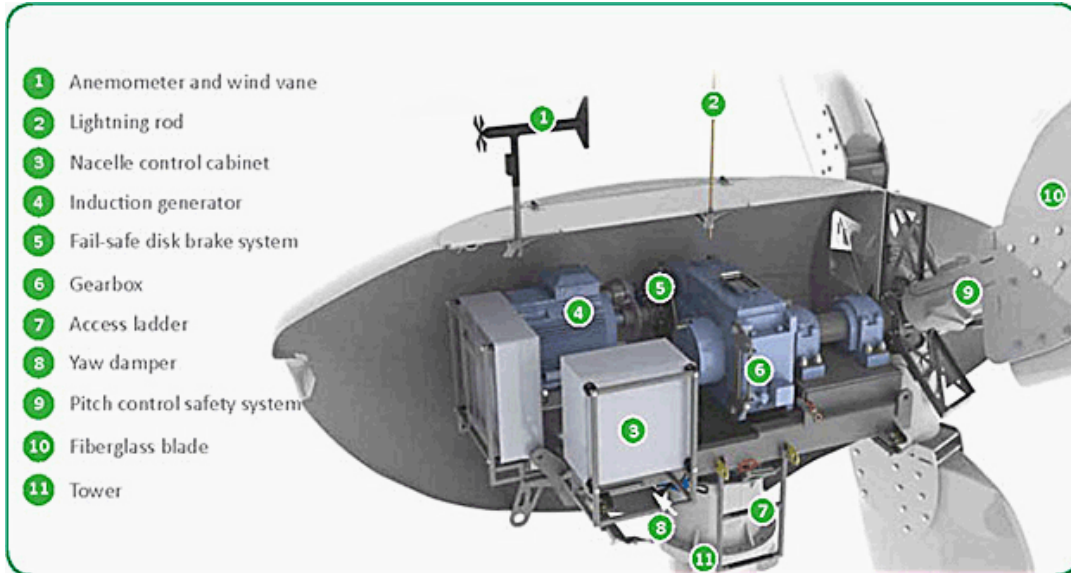
Is it
Sensitive



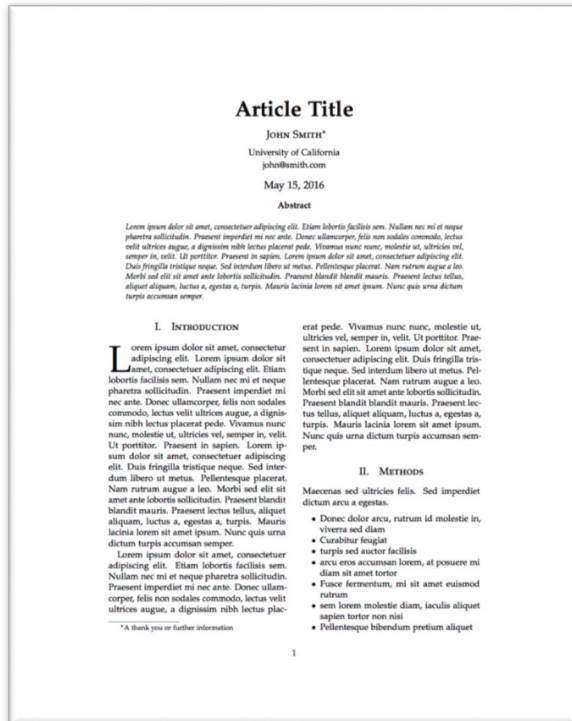
Gyroscopic control systems

Is it Sensitive

Turbine specifications



Is it Sensitive



Your Paper

Security != Privacy != Ethics

data Lifecycle

Storage?
Backup/Restore?
Speed?
Capital vs Operational?
Future Accessibility?
Consent Removal?
Sharing?
Retention Requirements?
Destruction Requirements?



Examining Security Components

- Governance
- Operations
- Response



Confidentiality

Integrity

Availability



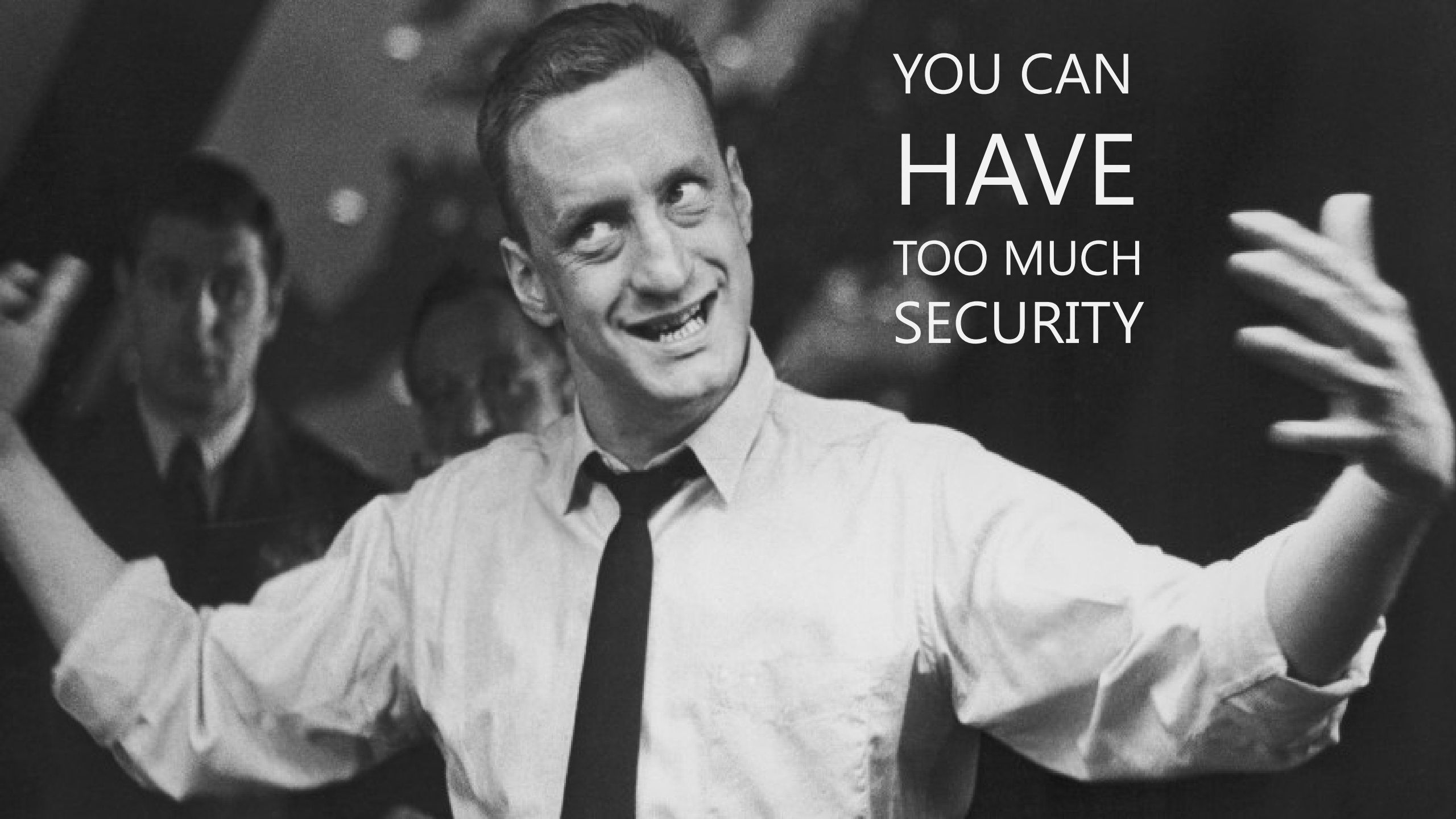
HOW I
LEARNED
TO STOP
WORRYING
AND
LOVE IT
SECURITY



HACKERS
BREACHES
AND THREATS
OH MY!

THERE IS
NO
SILVER
BULLET





YOU CAN
HAVE
TOO MUCH
SECURITY

PASSWORDS
ARE
PAINFUL





FOLLOW
INSTITUTIONAL
RULES

PAYING
ATTENTION
VS PARANOIA



THINK
BEFORE YOU
CLICK





WHO
ARE YOU
TRUSTING



General Principles

- Security is C.I.A - it's not just C
- Every layer helps... Up to a point
- Concept of trust
 - Who am I trusting with what?
- Prioritize
- You are a layer (social engineering)
 - Think before you click
 - Audit yourself
- Keep up to date with news
 - Keep informed rather than overwhelmed

HERE ARE
SOME
ACTION ITEMS



paws for
Questions?





Internet of Things



Social Media



"Cloud"



Overarching



Mobile

Implementation

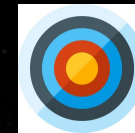
How hard?

Interference

How Painful?

Improvement

What sort of Impact?



What



Why



How

Resources

- Brave Browser: <https://brave.com/>
- KeePass Password Safe: <https://keepass.info/download.html>
- Cryptomator: <https://cryptomator.org/>

- Browser Add-ins:
 - uBlock Origin Chrome & Brave: <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>

🎯 Unique Passwords (Secrets)

❓ The single most important good habit:
Prevent one site's breach from exposing all your accounts.

💬 Remember how to build passwords rather than trying to memorize passwords or use a password manager (or both!)

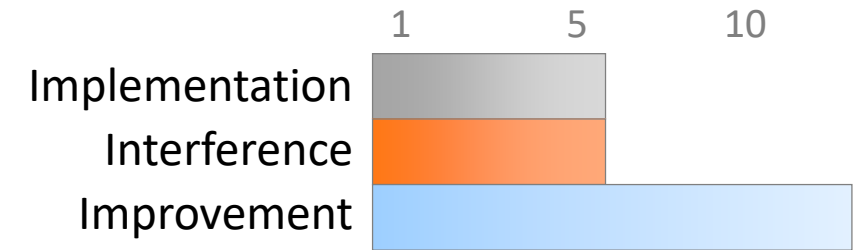
Size matters – use passphrases

Your key-pair should also be unique.

Only change them when necessary

Do not allow browsers to “memorise passwords”

<https://haveibeenpwned.com/>



Bonus Tip:

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



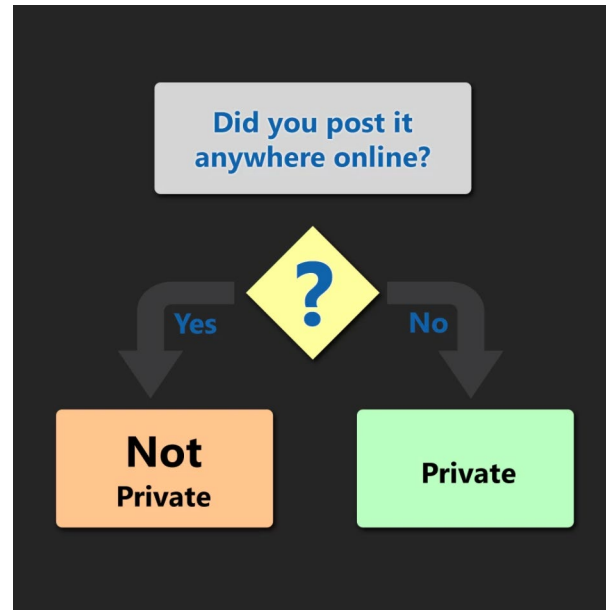
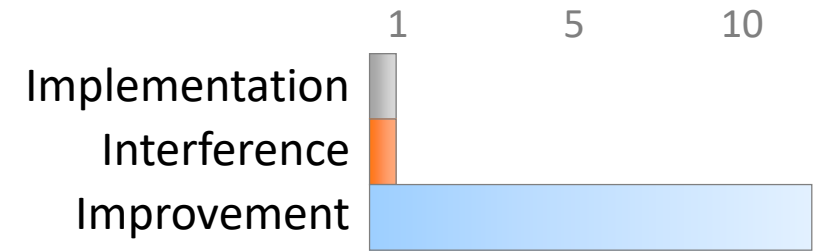
Sharing and Privacy

? 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 if it helps promote safe sharing behaviour.



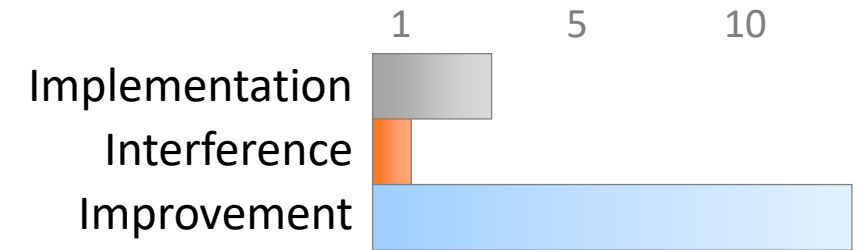
Delete Unnecessary Information

 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:

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



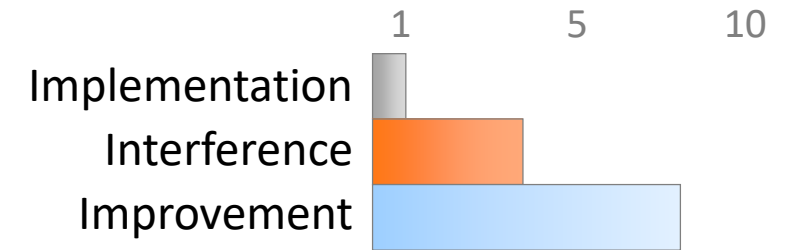
🎯 Don't Copy and Paste Code

❓ 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.



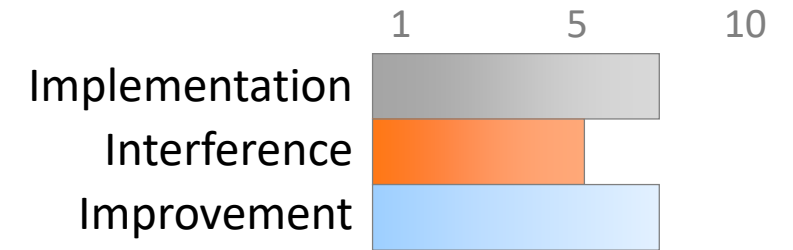
Supply Chain Trust

? If we don't know what is in the software, how do we trust it.

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

Use the minimal set of libraries, frameworks, and dependencies.

Sometimes custom written code is actually faster and more efficient.



Bonus Tip:

Diff library updates to see what changed.



🎯 Use Multi-Factor Authentication

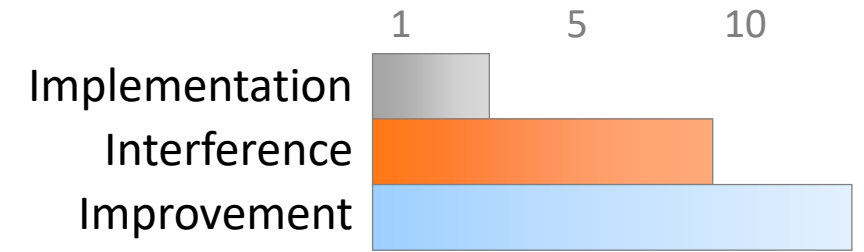
❓ Passwords are a single point of failure.
MFA therefore provides dramatically increased protection.

🗨️ Something you Have, Know, or Are

SMS is insecure, but still better than nothing

Many options exist, many systems support it.

EG: YubiKey, Google Authenticator, SecurID, etc...



Bonus Tip:

Also avoid social media single sign on to prevent creating a back door on yourself



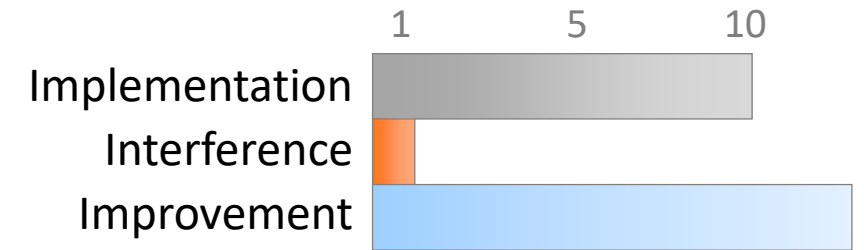
🎯 Have Backups and Plan to Restore

❓ 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.





Bonus Tip:

Test your restoration plan periodically – ensure it works.



Reset Default Passwords

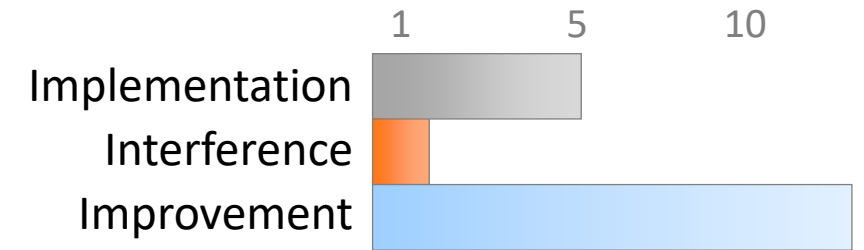
 Mitigates bots / scripted compromise
Easier for you to access

 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 needs to have 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!



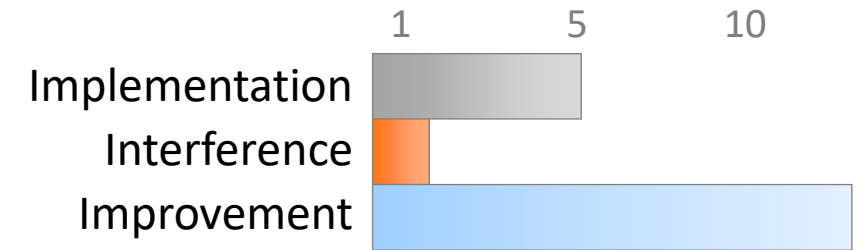
🎯 Protect any Recovery/Reset Pathways

❓ Password reset/recovery can bypass all other security
You put in place with good passwords and MFA

💬 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.

Consider establishing different recovery information for different
accounts.





Bonus Tip:

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



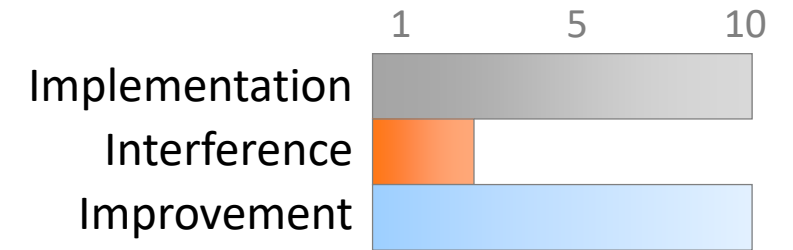
Use a VPN

-  All unencrypted traffic over a network is subject to snooping
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)

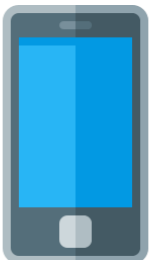
<http://www.pcmag.com/article2/0,2817,2403388,00.asp>

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.



Authenticate to Unlock

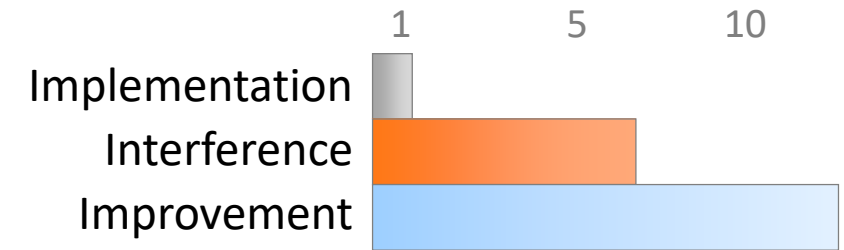
 An unlocked device in the wrong hands has full access to everything you normally do.

 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.

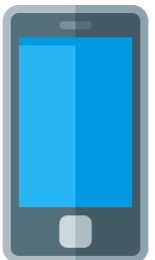
If using a PIN avoid "guessable" items (dates, phone numbers etc)

Keep your screen clean to avoid telltale fingerprints.



Bonus Tip:

Biometric unlocks may be fooled or broken entirely.



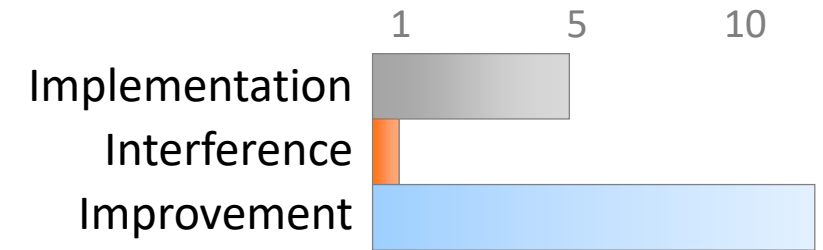
Identity Theft

? 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.

Google 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.



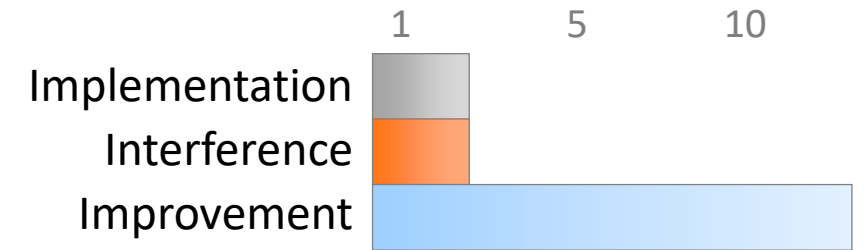
Power Off

 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.

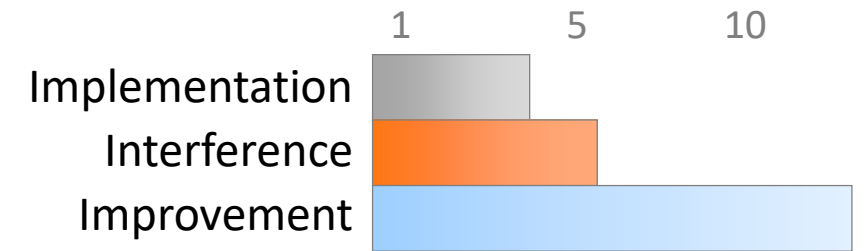


Security Questions & Answers

-  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 must 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.



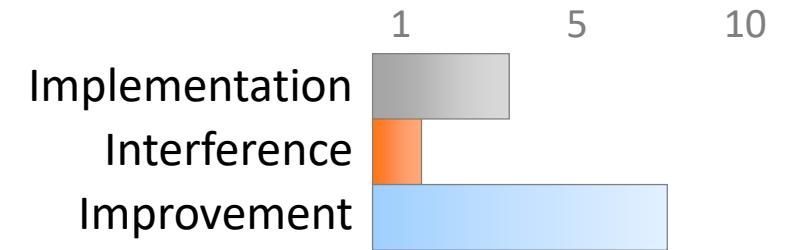
🎯 Apply Software Updates

❓ 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 rely on automatic updates.




Bonus Tip:

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

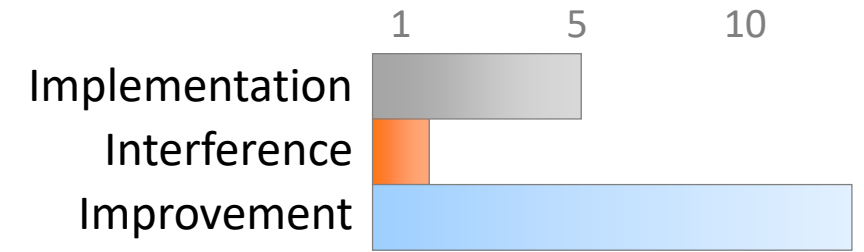


Cameras/Microphones can Record

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

 Tape over 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.



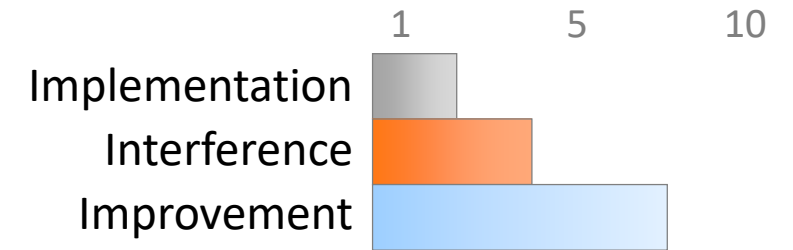
🎯 Block Ads, Flash, Trackers

❓ Flash is riddled with security holes, ads 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.



Keep Recovery Information Secure

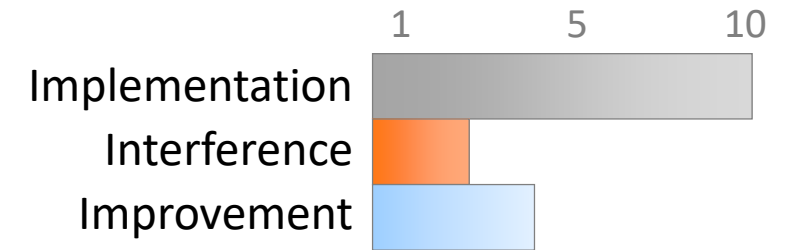
? This can be the weakest link in the chain, the password is useless If someone has your recovery information.

Always consider what information is used as recovery for an account. If this is easy to guess or infiltrate than it can be used to compromise the account your are protecting.

Set up unique emails for different services (do not forward all these to the same location).

Keep recovery MFA keys safe and locked away.

Periodically review recovery procedures/information for services.



Bonus Tip:

Some experts recommend a special phone number only used for recovery.



🎯 Be wary of USB

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

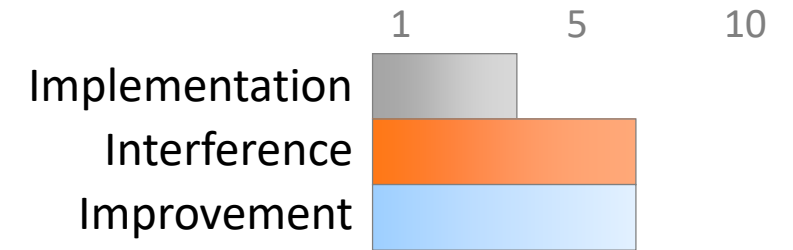
💬 Turn off auto-everything for USB devices and learn how to prevent auto-launching if your OS supports it.

Do not use “found” or “free” USB keys unless you 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.

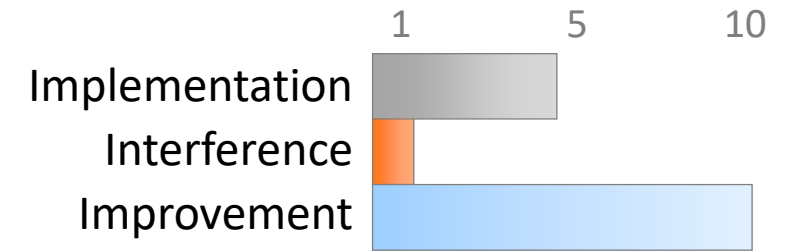


🎯 Encryption at Rest

❓ 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.

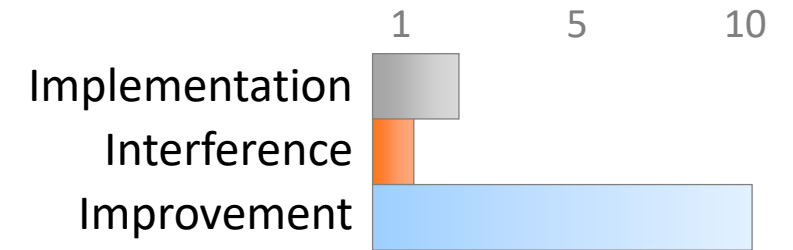


Shoulder Surfing

 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

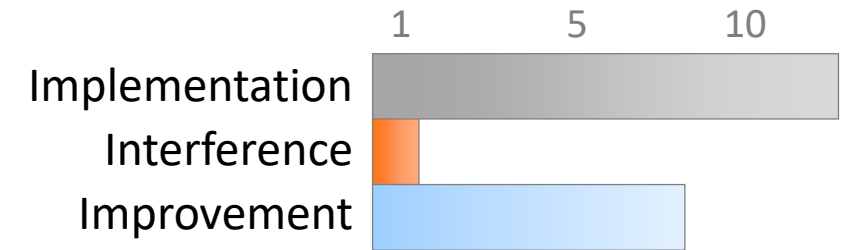


🎯 Segment your IOT devices

❓ A more restricted separate network 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.



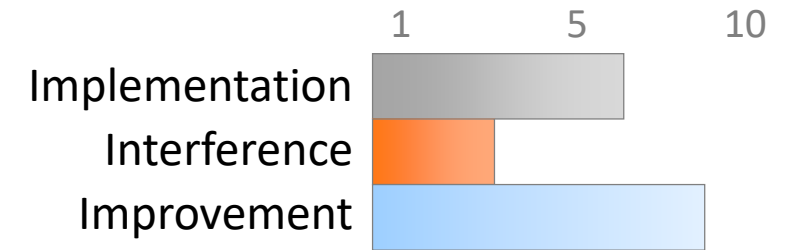
Audit Authorized Apps

 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.



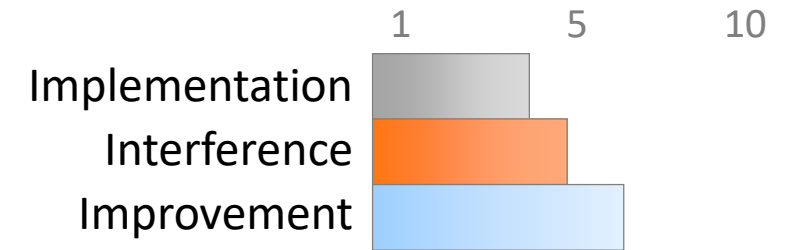
Photo Sharing – Hidden Data

? 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)

Expect shared photos to be stolen and 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.



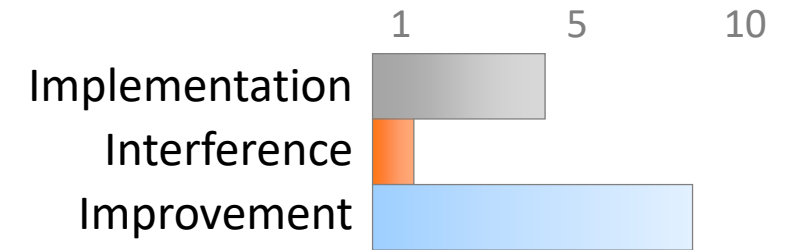
Audit Shared Folders

 Ensures only currently trusted people have access
Reduces 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 not required.



Bonus Tip:

This can save space on your hard drive as well.



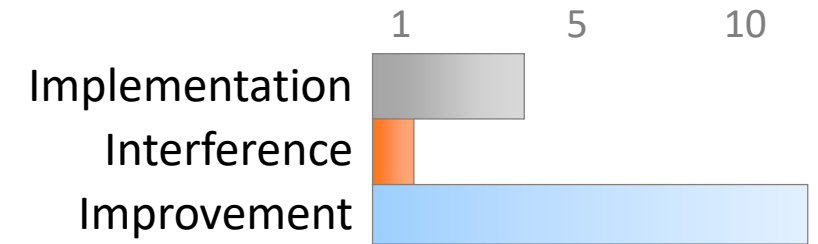
Sanitize before Disposal

? 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.



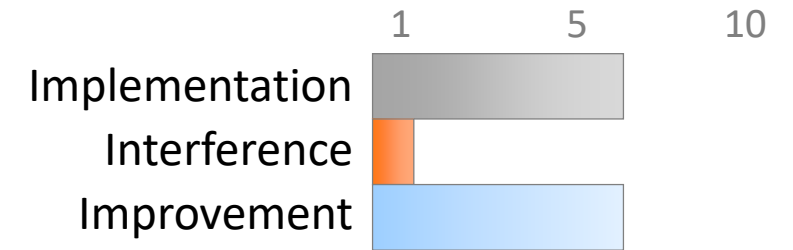
Securely Delete Files (Cloud)

? 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.

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.



🎯 Use Encryption (cloud/file)

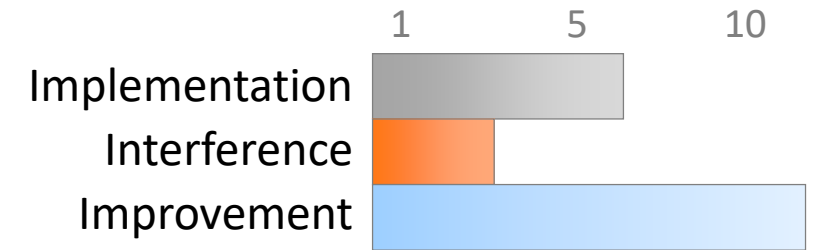
❓ Encrypting data adds protection both in transit and at rest, usually adding an additional layer of security.

💬 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 options for encryption that automate the process but require special software:

<https://cryptomator.org/> (free option)

<https://www.boxcryptor.com/> (commercial)



Bonus Tip:

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



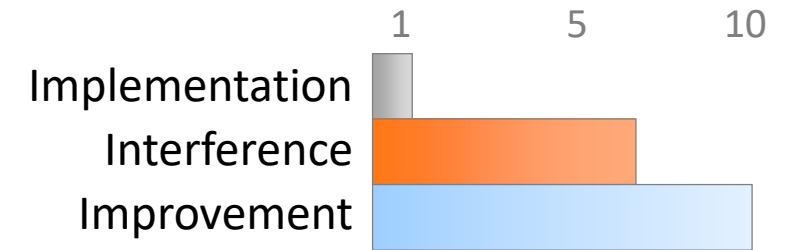
🎯 Enable Quick Auto-Lock

❓ 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).

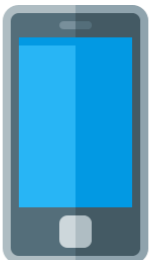
Consider changing the duration based on current risk (at home vs at a conference)

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!



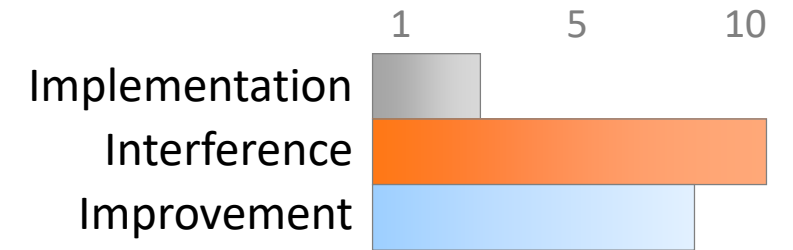
Sign-out

 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.

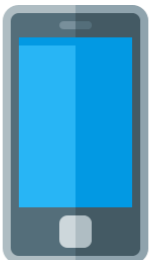
Signing out adds another layer of security.

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.

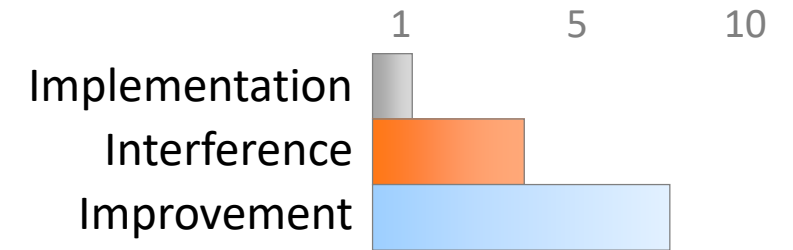


🎯 Avoid Lock-Screen Disclosure

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

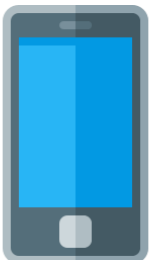
☰ Ensure phone settings prevent the display of content like text messages, email, notifications directly on the locked phone.

When many services use a SMS code to reset a password – 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!



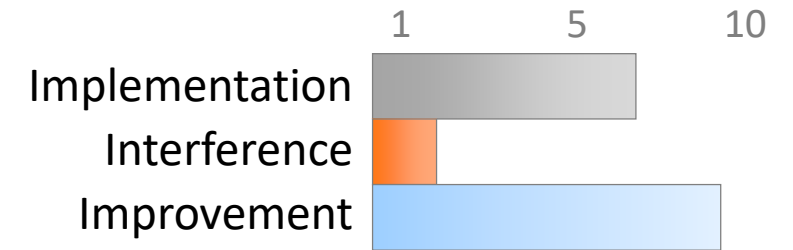
Guest infections through WiFi

 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 can 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.

