

GO

Ready?



42%

THINK

|||||

|||||



Tips, Tricks,
Tools, & Threats...

In: IT, AI, and Research Security

A Universe of

IT

tricks and tips...



(it's only a model)

My first computer...

Heathkit H88: Home-bult computer ~ Circa 1979



No network, No storage, No software, 8K RAM
and... User serviceable parts! (well, kinda)

Heathkit H88: Home-bult computer ~ Circa 1979



Ya, I've been at this a while...




Troubleshooting



Turn it **OFF**

&

Turn it back
ON again



Less Extreme

Troubleshooting

ONLY change one thing at a time

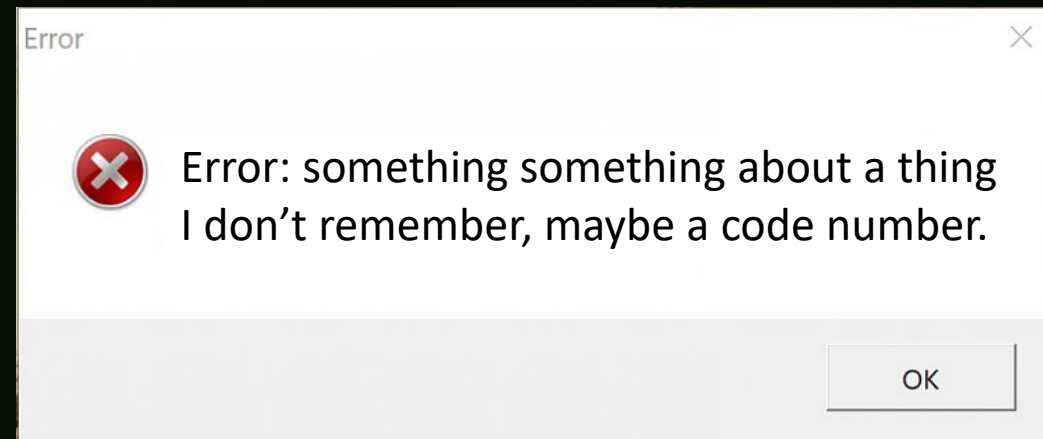


Tech Support: “Was there any error?”

Client: “Yes!”

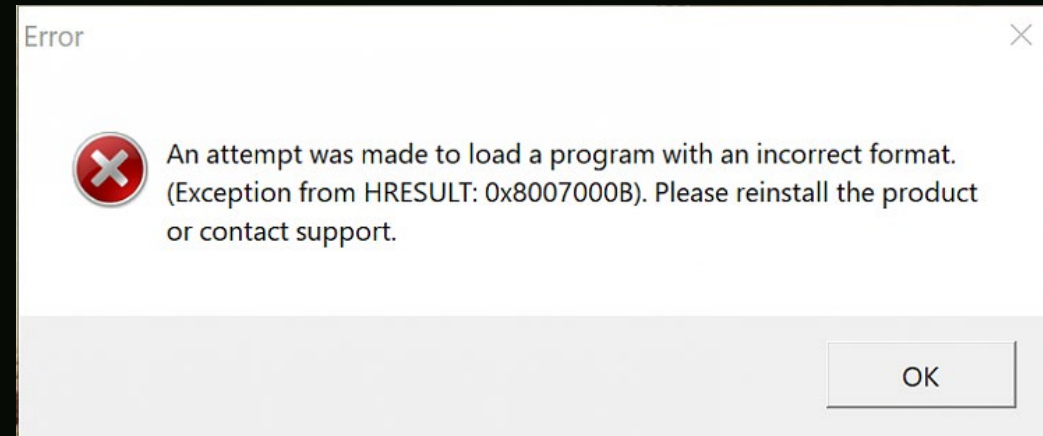
Tech Support : “Great, what did it say?”

Client : “err.....”



Screenshot Error Messages

Keep notes



More detail = Faster resolution



More
Troubleshooting

How to Disable or Remap Caps Lock Key in Windows

The caps lock key is one of those remnants of another age of computers, back when people used to shout at each other more often. Unless you're in the

5 Ways to Turn Off or Disable Caps Lock on Any Keyboard

▶ Videos



How to Permanently
Disable Caps lock Key in
Windows

3K views

▶ YouTube 9mo



How to disable the Caps
Lock key in Windows® 7

31K views


▶ YouTube 11yr

How to Disable or Remap Caps Lock Key in Windows

The caps lock key is one of those remnants of another age of computers, back when people used it out at other more often. Unless you're in the

5 Ways to Turn Off or Disable Caps Lock on Any Keyboard

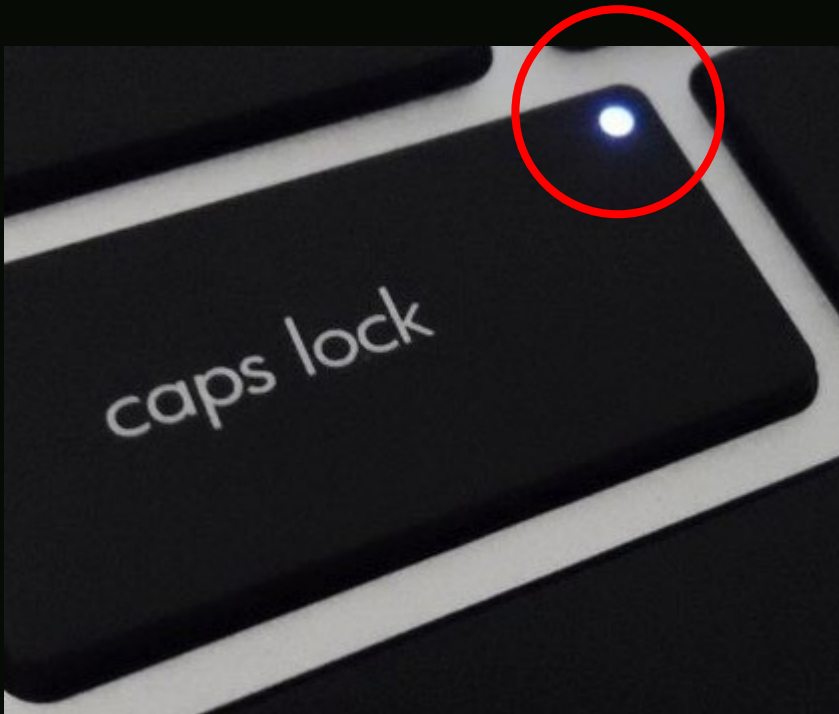
▶ Videos



How to Permanently Disable Caps Lock Key in Windows
3K views
YouTube 9mo

How to disable the Caps Lock key in Windows® 7
31K views
YouTube 11yr

Caps lock is actually a troubleshooting tool:



For the light to toggle, keyboard interrupts must work. Meaning, your computer is still responding at the CPU level.

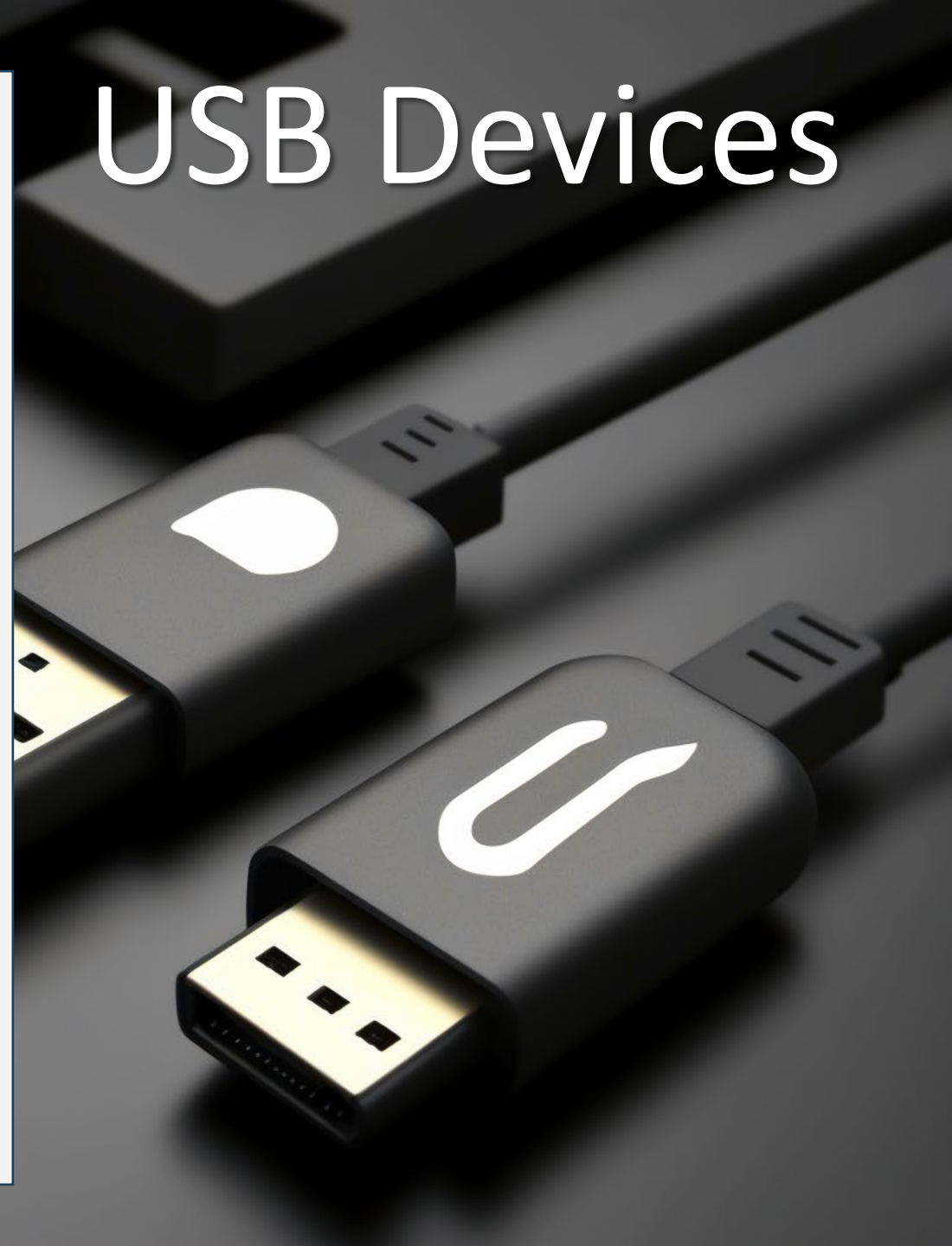
If the light doesn't toggle... "It's dead Jim."

USB Devices



USB Devices

Try a different cable
Try a different port
Unplug all the things
Use quality cables



USB Devices

- Try a different cable
- Try a different port
- Unplug all the things
- Use quality cables



<https://www.lumafield.com/article/usb-c-cable-charger-head-to-head-comparison-apple-thunderbolt-amazon-basics>



USB C port, cleaning tool:



USB Formatting:



- FAT (FAT32): Max 4GB File, Old, Great Compatibility
- ExFAT: Max 128PB File, New, Reasonable Compatibility
- NTFS: Max 8PB File, Windows Only

Format sbaker16G (D:) [X]

Capacity: 14.6 GB

File system: exFAT

Allocation unit size: 32 kilobytes

Restore device defaults

Volume label: sbaker 16G

Format options: Quick Format

Start Close

Name the drive with its size and something to help reclaim it if lost. EG: at a conference.



Shortcuts



Sorry Mac/Linux users...



Please
Consult the duck

<https://duckduckgo.com/>

Key Combinations



L

Lock



M

Minimize All



.

Emoji

Alt Tab

Cycle Applications

Ctrl W

Close Tab

F5

Reload

Ctrl Shft Esc

Task Manager



Windows Tips

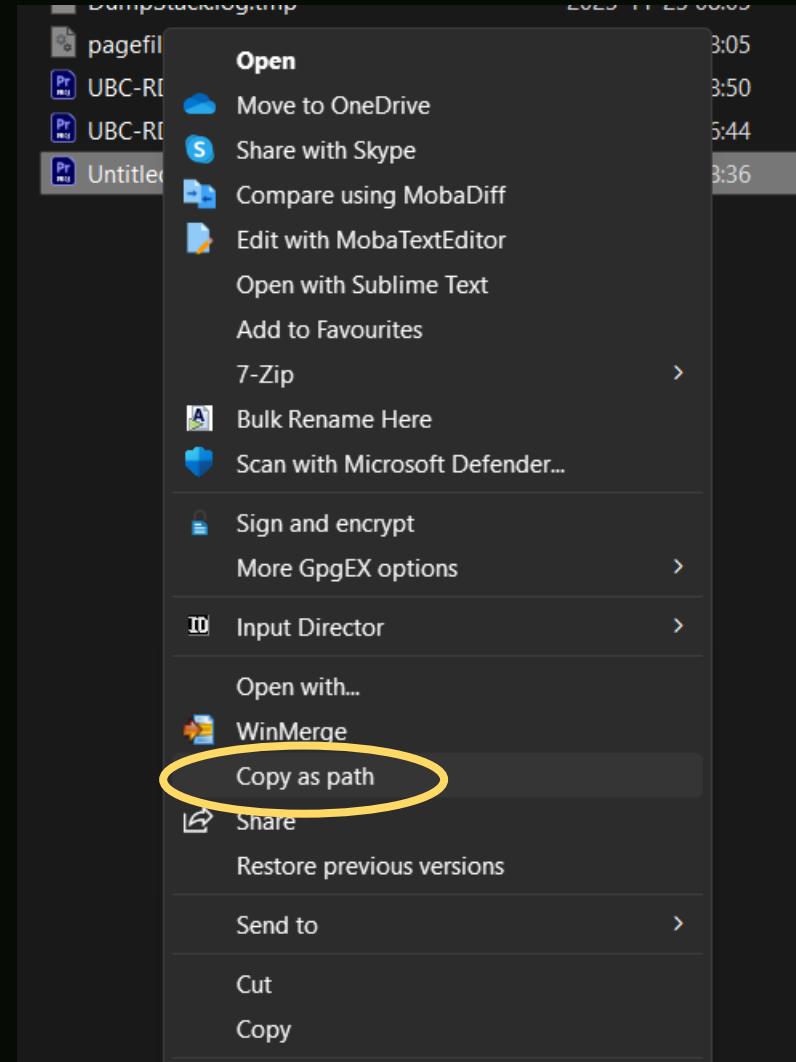
Right Click

Copy as path

"E:\Untitled.prproj"

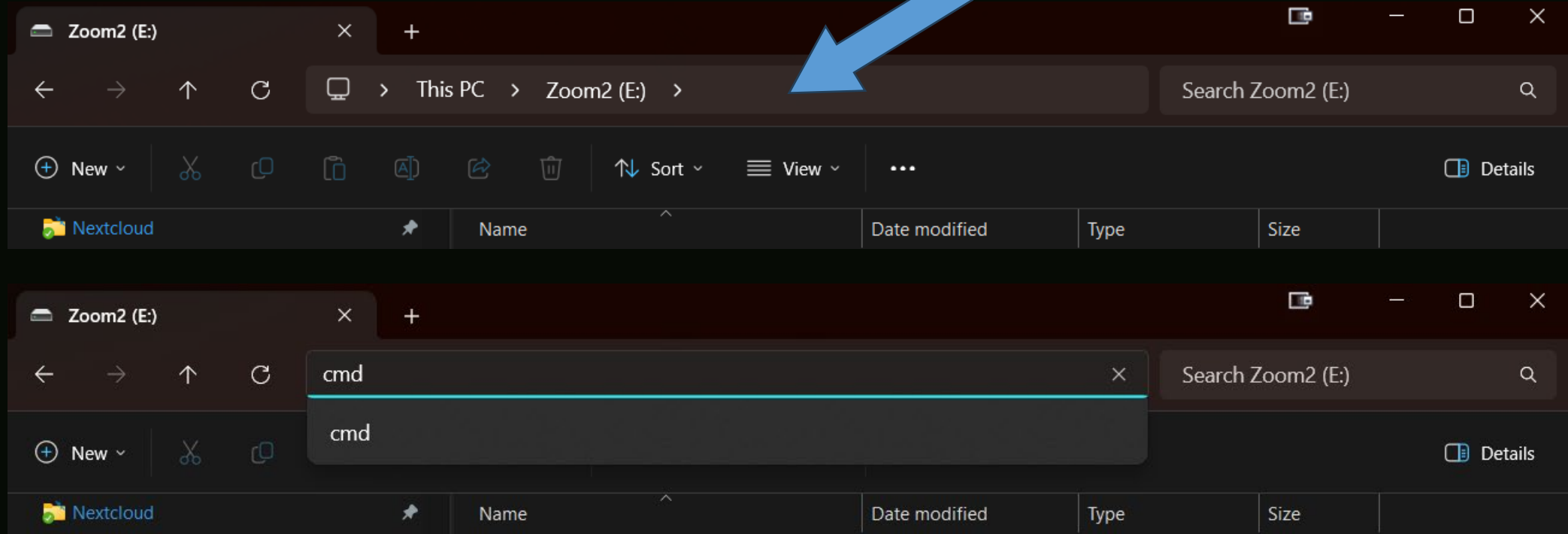
Works for Network paths/files too:

"\\nas3\data\Downloads\ITIL\13 - Availability Management.wmv"



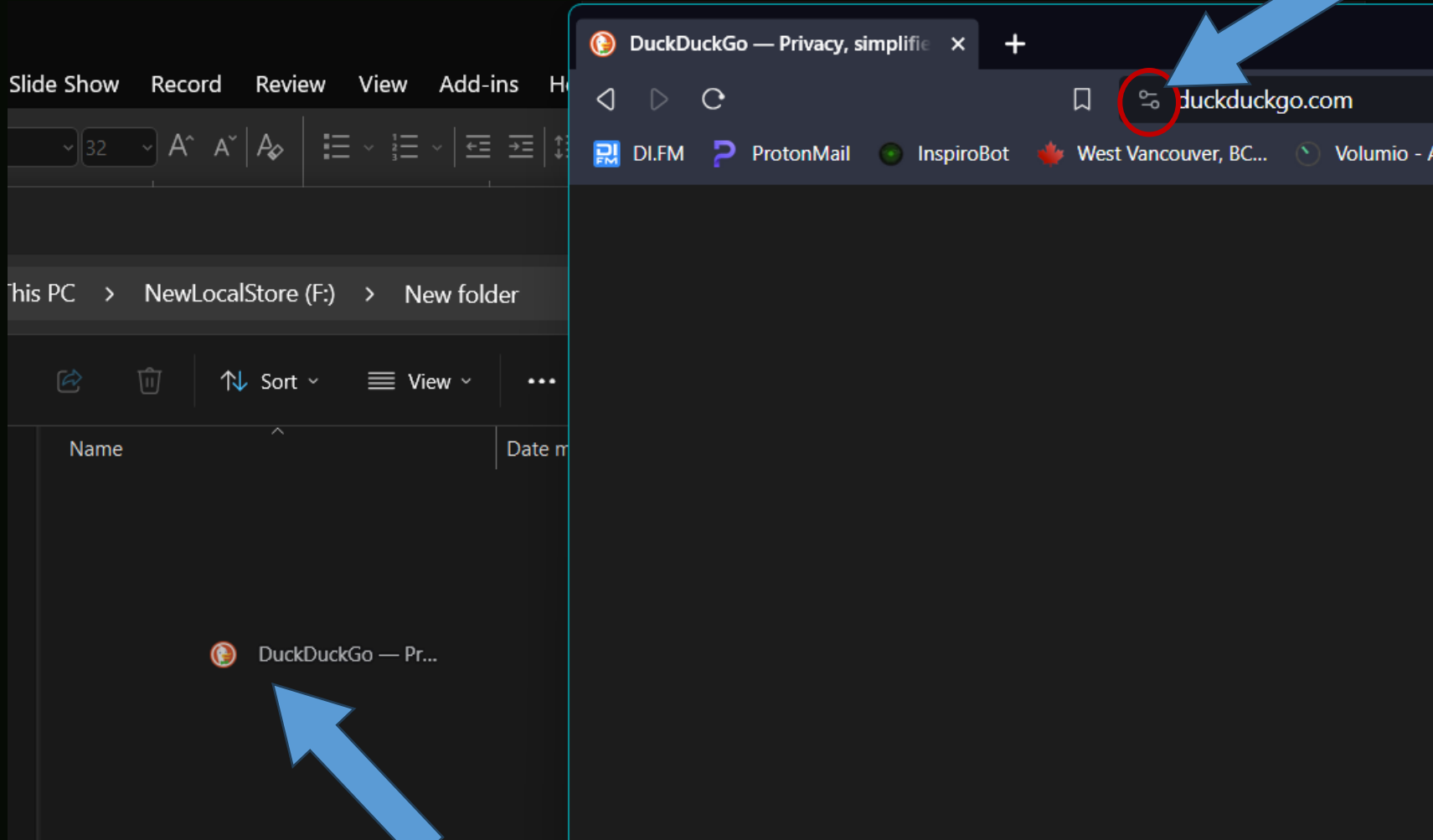
Run Program in Folder

CLICK



Drag & Drop Web Shortcuts

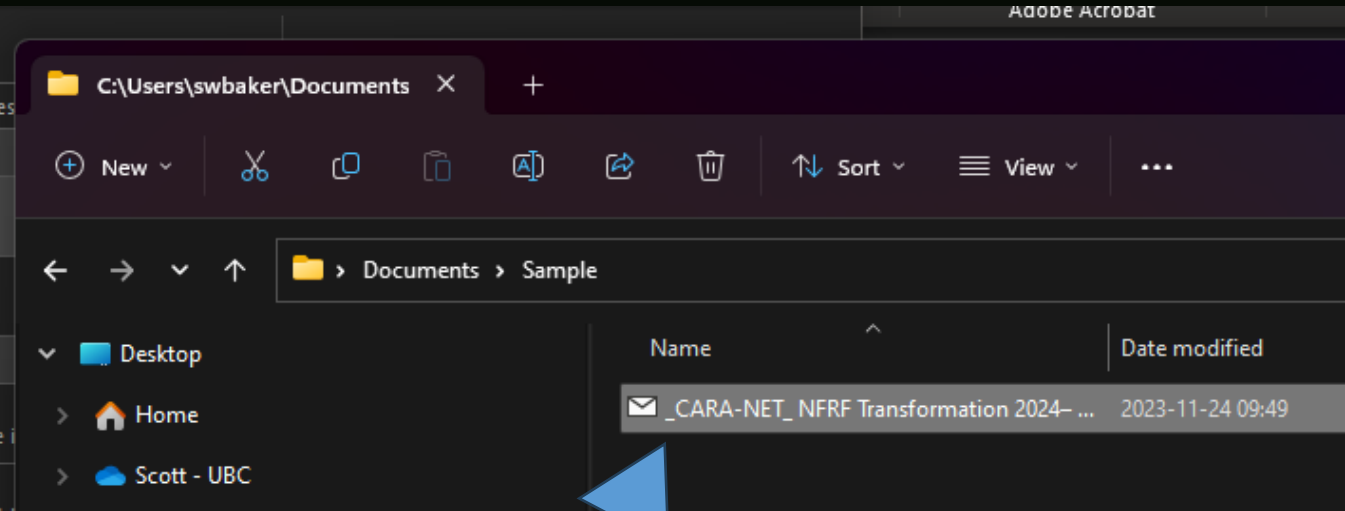
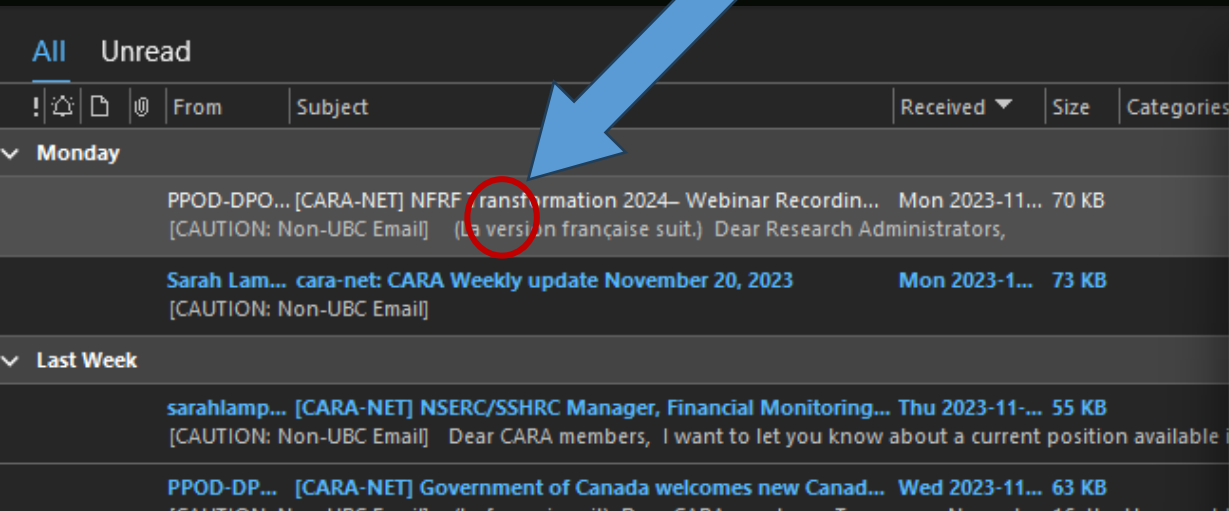
Click & Drag



Drop

Email drag to File

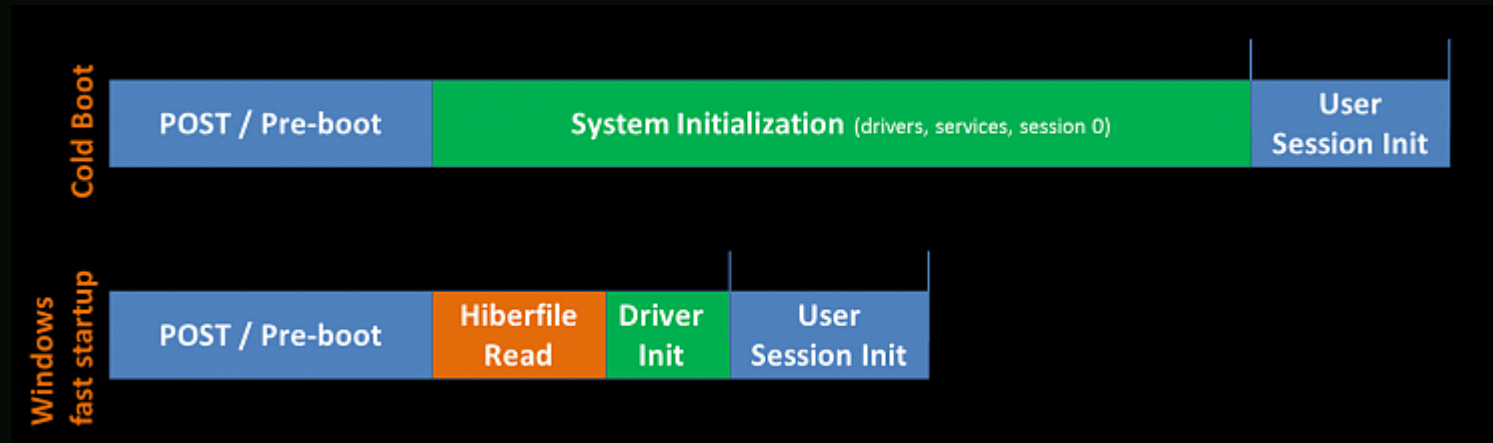
Click & Drag



Drop

Restart vs Shut-down/Power on

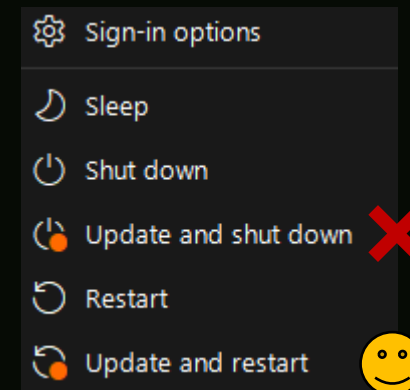
Probably the opposite of what you think!



If you disable **hibernate**, it will also disable fast startup.

Look in C:\

hiberfil.sys	2023-11-24 07:13	System file	6,595,808 KB
--------------	------------------	-------------	--------------





Software

ValiDrive

<https://www.grc.com/validrive.htm>



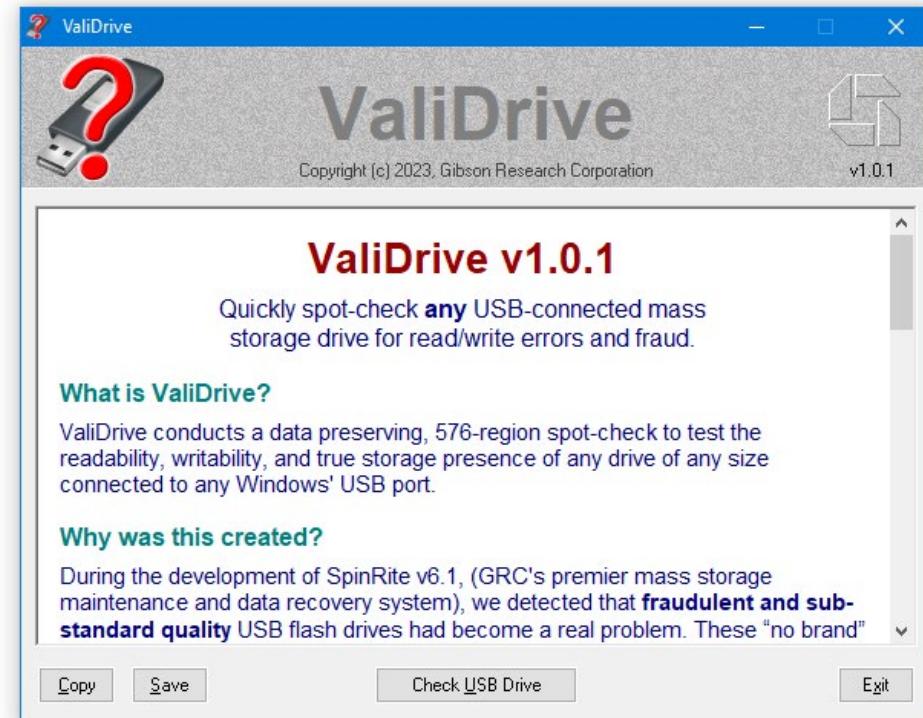
All Fake

Again, you get what you pay for.



ValiDrive

Quickly spot-check any USB mass storage drive for fraudulent **deliberately** missing storage.



Ninite

<https://ninite.com/>

1. Pick the apps you want

Web Browsers

- Chrome
- Opera
- Firefox
- Edge

Documents

- Foxit Reader
- LibreOffice
- SumatraPDF
- CutePDF
- OpenOffice

Online Storage

- Dropbox
- Google Drive for Desktop
- OneDrive
- SugarSync

Messaging

- Zoom
- Discord
- Skype
- Pidgin
- Thunderbird
- Trillian

Security

- Essentials
- Malwarebytes
- Avast
- AVG
- Spybot 2
- Avira
- SUPERAntiSpyware

Developer Tools

- Python x64 3
- Python 3
- Python

Media

- iTunes
- VLC
- AIMP
- foobar2000
- Winamp
- MusicBee
- Audacity
- K-Lite Codecs
- GOM
- Spotify
- CCCP
- MediaMonkey
- HandBrake

Utilities

- TeamViewer 15
- ImgBurn
- RealVNC Server
- RealVNC Viewer
- TeraCopy

Runtimes

- Java (AdoptOpenJDK) x64 8
- Java (AdoptOpenJDK) 8
- Java (AdoptOpenJDK) x64...
- Java (AdoptOpenJDK) x64...
- Java (AdoptOpenJDK) x64...
- .NET 4.8
- .NET Desktop Runtime x64 5
- .NET Desktop Runtime 5
- .NET Desktop Runtime x64 6
- .NET Desktop Runtime 6
- .NET Desktop Runtime x64 7
- .NET Desktop Runtime 7

Other

- Evernote
- Google Earth
- Steam
- KeePass 2
- Everything
- NV Access

Imaging

- Krita
- Blender
- Paint.NET
- GIMP
- IrfanView
- XnView
- Inkscape
- FastStone
- Greenshot
- ShareX

File Sharing

- qBittorrent

Compression

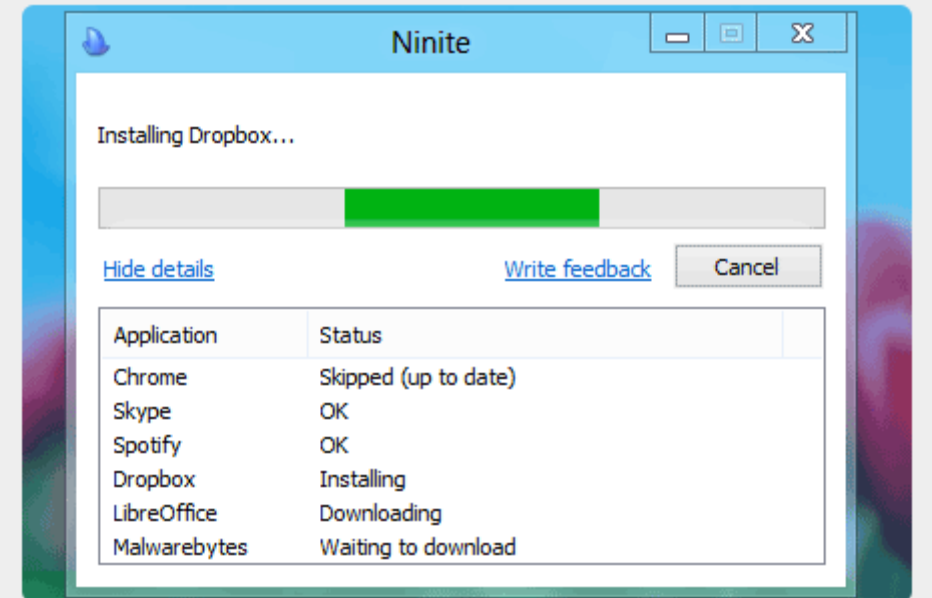
- 7-Zip
- PeaZip
- WinRAR

Update all the things!



Install and Update All Your Programs at Once

No toolbars. No clicking next. Just pick your apps and go.



Input Director

<https://inputdirector.com/>



Free Software KVM

Input Director

Clients

Systems that can be directed from this computer

Skip	Status / Name	Port	Hotkey
<input type="checkbox"/>	✓ bob	31234	
<input type="checkbox"/>	✓ jane	31234	

Default all systems to 'skip' on startup

Drag and resize the icons to match the physical arrangement of the systems monitors

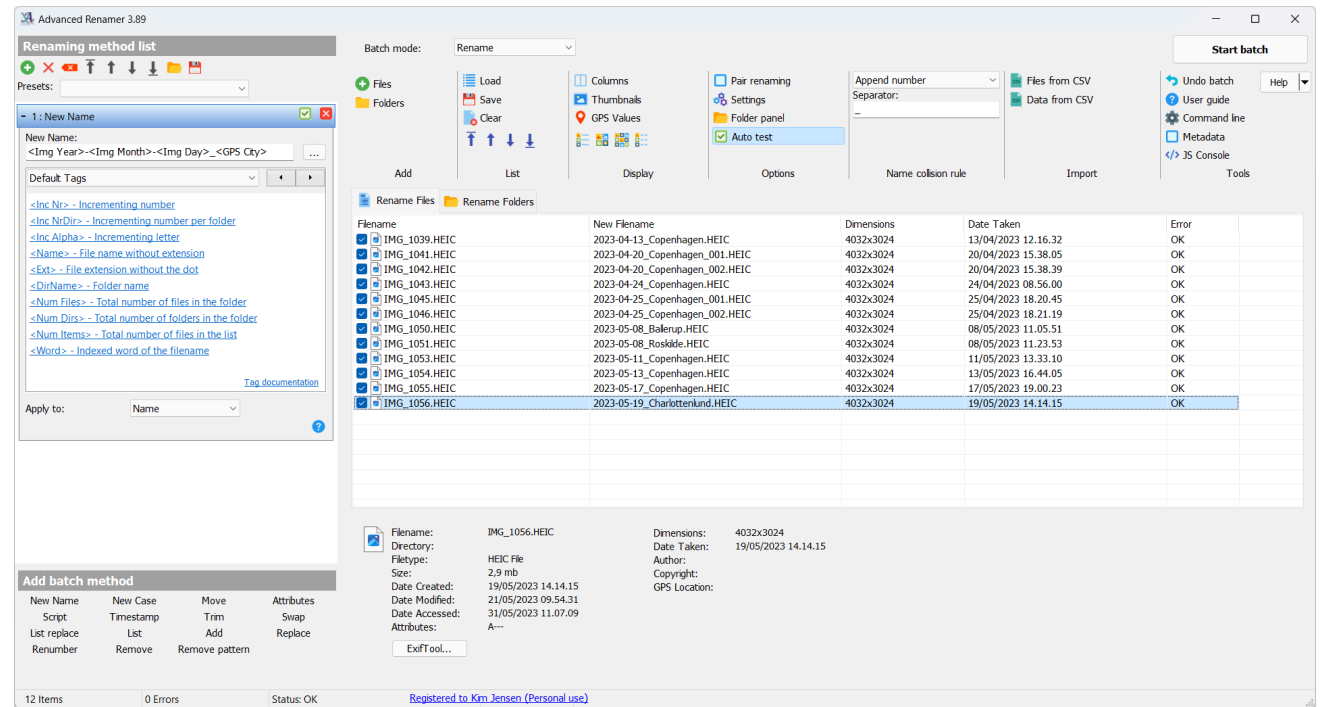
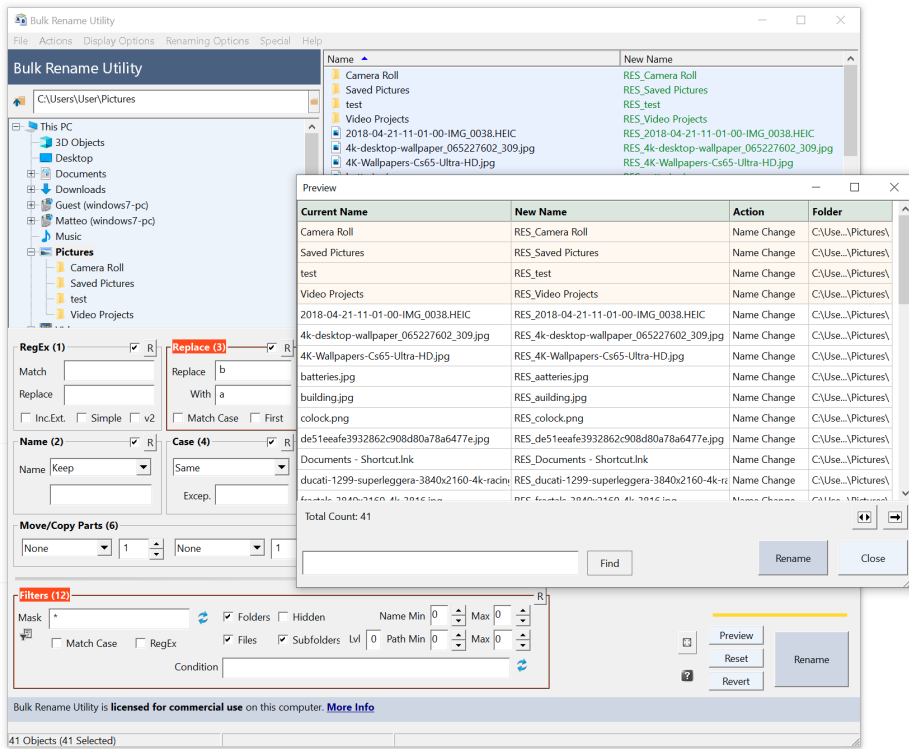
Director Monitor Setup

Cursor Wraparound

Bulk Rename or Advanced Renamer

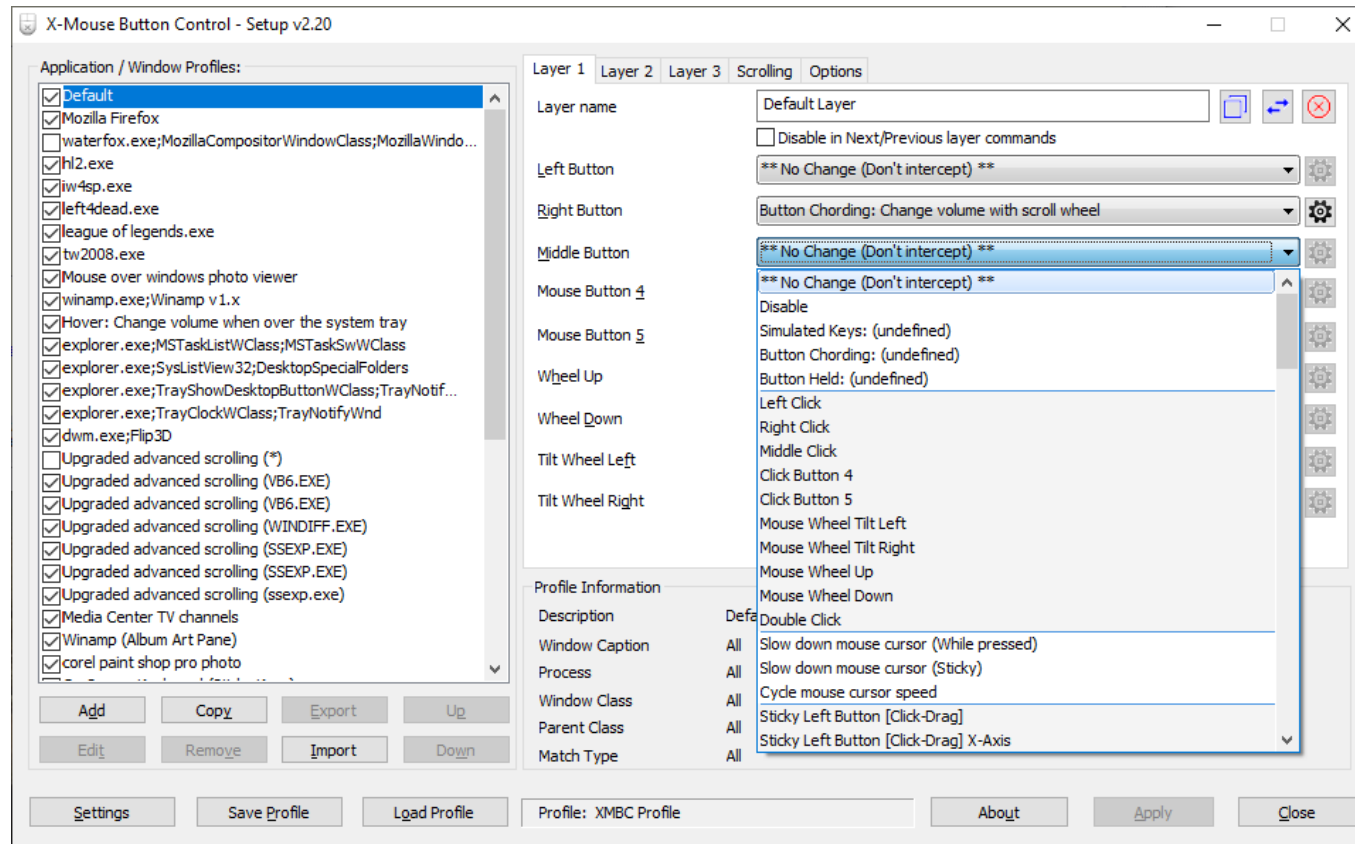
<https://www.bulkrenameutility.co.uk/>

<https://www.advancedrenamer.com/>



X-Mouse Button Control

<https://www.highrez.co.uk/downloads/XMouseButtonControl.htm>





Remap mouse buttons, add macros, and adjust scrolling per application.



Cybersecurity

eTransfer Autodeposit

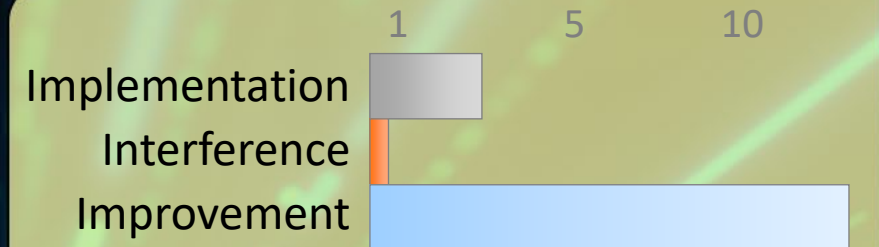
 Register your email for autodeposit with eTransfers.

 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

Keep Work and Personal Identities Separate

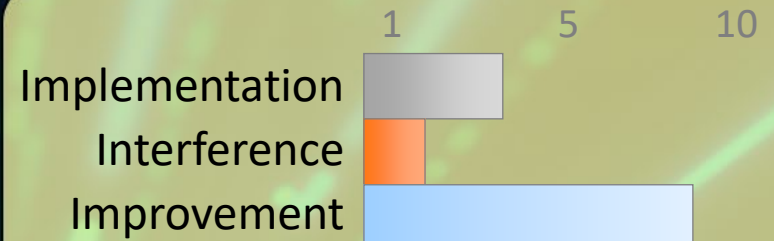
 Your business contact information is public
Your personal contact information is private

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

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 because of that.



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

Multiple Browsers

 Use different browsers for different purposes.

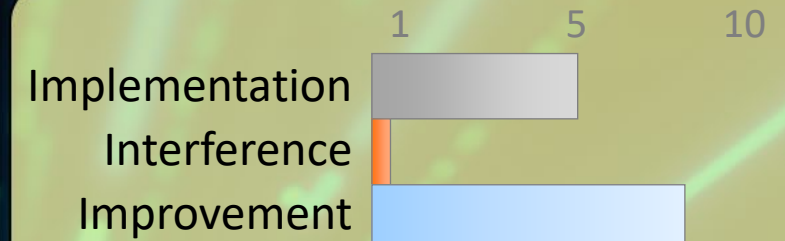
 Reduces Tracking

Reduces risk “wrong account”

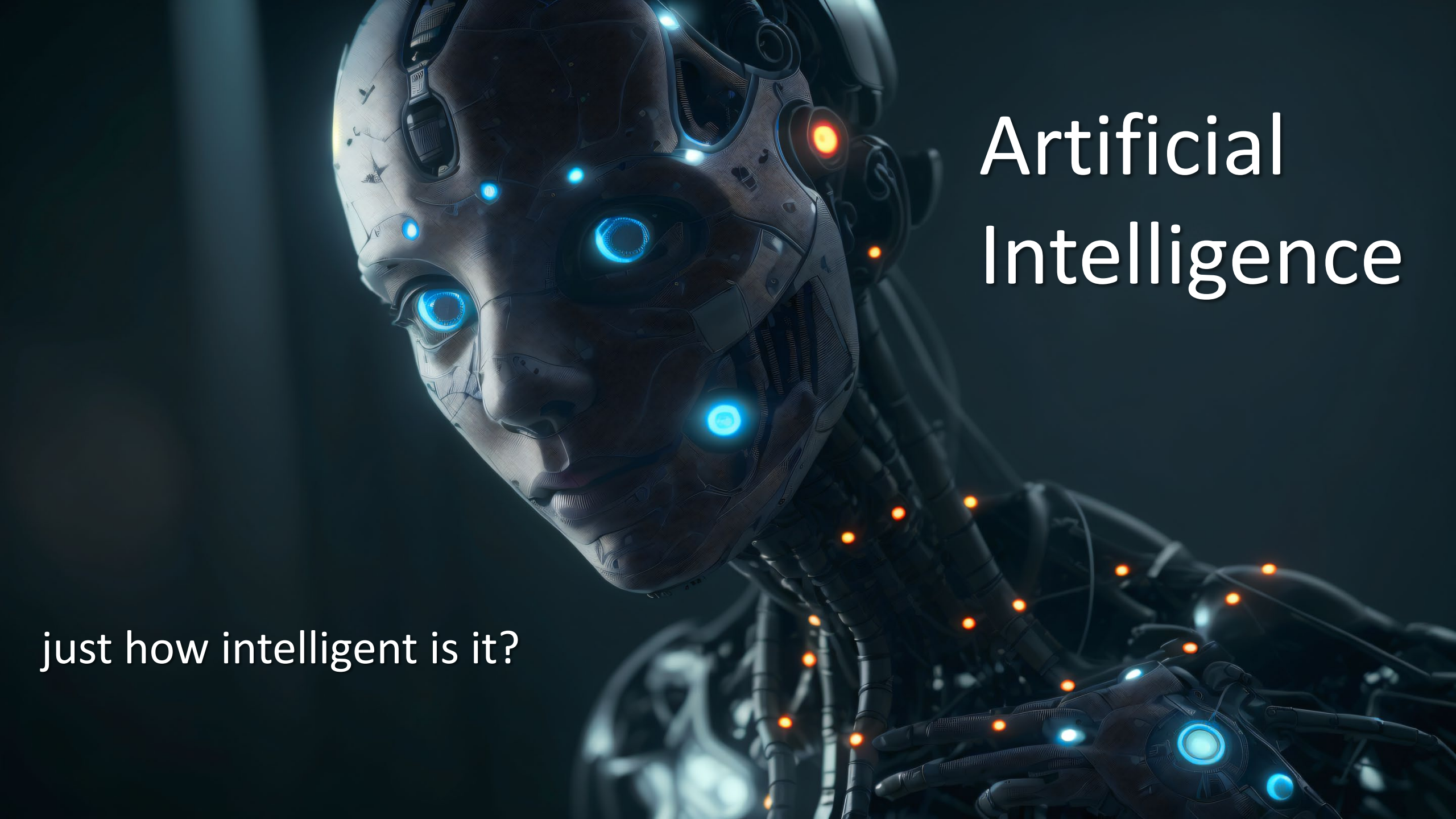
Allows for reduced extensions in the browser used for higher risk activities.

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.



Artificial Intelligence

just how intelligent is it?

An open book with a magnifying glass resting on it. The word "Terminology" is written in a large, bold, black font across the center of the magnifying glass's lens. The background shows the pages of the book with faint, illegible text.

Terminology



Artificial Intelligence (AI)
is big, really big...



Machine Learning
Still covers a lot...

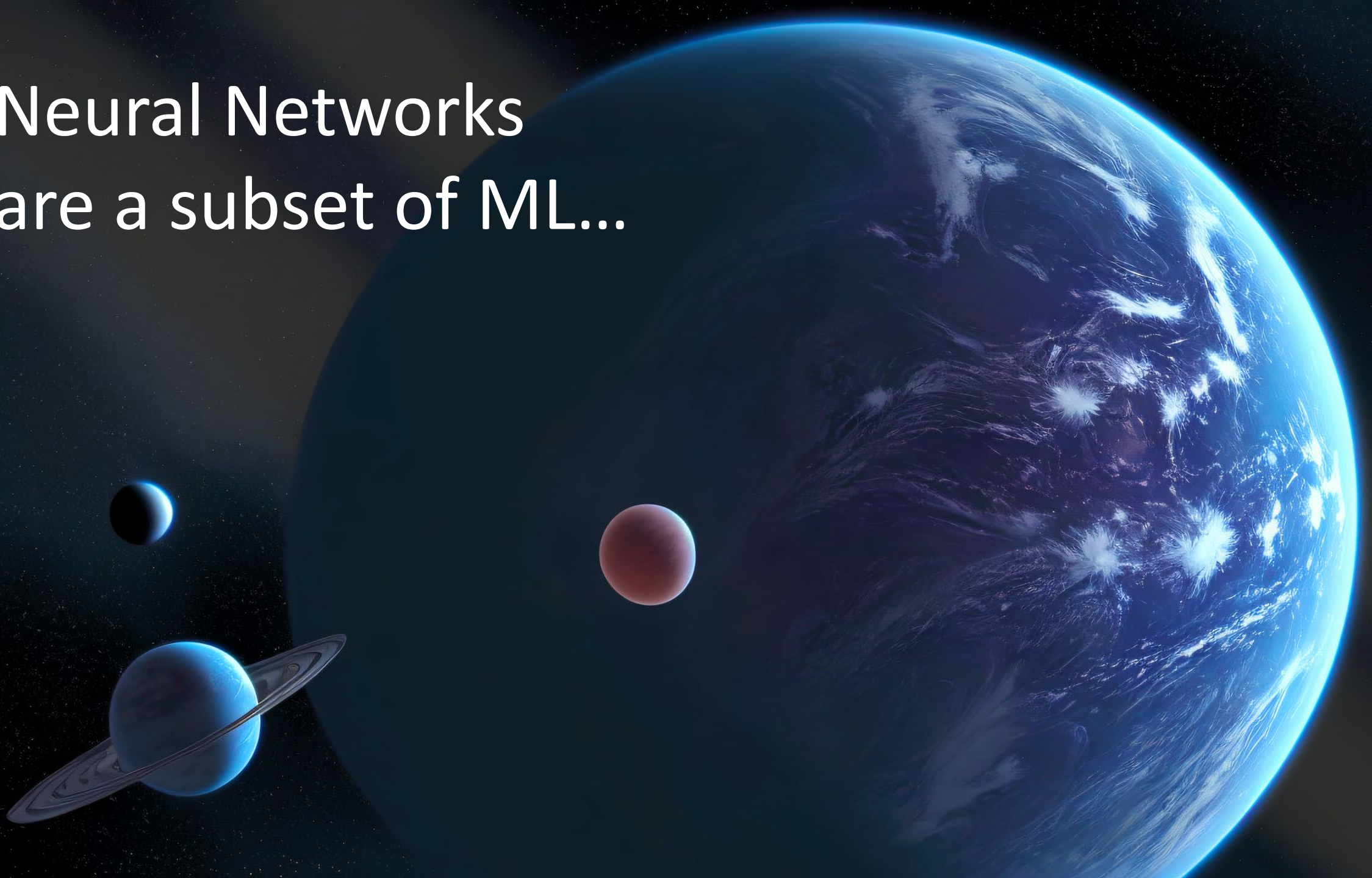
THE GREAT WALL

THE GREAT WALL

THE GREAT WALL

THE GREAT WALL

Neural Networks
are a subset of ML...



Deep Learning

Based on neural networks



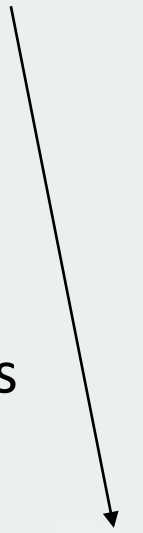
**Large
Language
Models
(LLM)**



Generative
Pre-trained
Transformers
(GPT)



ChatGPT



AGI - General Intelligence

(we do not have this)



ANI - Narrow Intelligence

(we have lots of this)



Generative – Creating output

Stable Diffusion checkpoint
aZovyaPhotoreal_v2.safetensors [5594efef1c]

Clip skip 1

SD VAE None

Tiling

txt2img img2img Extras PNG Info Checkpoint Merger Train Deforum Toolkit Tokenizer Wildcards Manager Settings

Rudolph the red nosed spider is afraid of pumpkins

Negative prompt (press Ctrl+Enter or Alt+Enter to generate)

Generation Textual Inversion Hypernetworks Checkpoints Lora

Sampling method DPM++ 3M SDE Karras

Sampling steps 20

Width 960

Height 540

Batch count 1

Batch size 4

Hires. fix Refiner

CFG Scale 7

Seed -1

Extra

Rudolph the red nosed spider is afraid of pumpkins



Generative – ~~Creating output~~ Transforming input

Stable Diffusion checkpoint
aZovyaPhotoreal_v2.safetensors [5594efef1c]

Clip skip: 1 | SD VAE: None | Tiling:

txt2img | img2img | Extras | PNG Info | Checkpoint Merger | Train | Deforum | Toolkit | Tokenizer | Wildcards Manager | Settings

Rudolph the red nosed spider is afraid of pumpkins

Negative prompt (press Ctrl+Enter or Alt+Enter to generate)

Generation | Textual Inversion | Hypernetworks | Checkpoints | Lora

Sampling method: DPM++ 3M SDE Karras | Sampling steps: 20

Width: 960 | Height: 540 | Batch count: 1 | Batch size: 4

Hires. fix | Refiner

CFG Scale: 7

Seed: -1 | Extra:

Rudolph the red nosed spider is afraid of pumpkins



Inference – Identifying input

txt2img img2img Extras PNG Info Checkpoint Merger Train Deforum Toolkit Tokenizer Wildcards Manager Settings Extensions

a spider sitting on top of a pile of pumpkins with eyes on it's legs and a pumpkin in the background, Chris LaBrooy, spooky, a stock photo, folk art

Negative prompt (press Ctrl+Enter or Alt+Enter to generate)

Generation Textual Inversion Hypernetworks Checkpoints Lora

img2img Sketch Inpaint Inpaint sketch Inpaint upload Batch

a spider sitting on top of a pile of pumpkins with eyes on it's legs and a pumpkin in the background, Chris LaBrooy, spooky, a stock photo, folk art

Inference – ~~Identifying input~~ Transforming input

txt2img **img2img** Extras PNG Info Checkpoint Merger Train Deforum Toolkit Tokenizer Wildcards Manager Settings Extensions

a spider sitting on top of a pile of pumpkins with eyes on it's legs and a pumpkin in the background, Chris LaBrooy, spooky, a stock photo, folk art

Negative prompt (press Ctrl+Enter or Alt+Enter to generate)

Generation Textual Inversion Hypernetworks Checkpoints Lora

img2img Sketch Inpaint Inpaint sketch Inpaint upload Batch

a spider sitting on top of a pile of pumpkins with eyes on it's legs and a pumpkin in the background, Chris LaBrooy, spooky, a stock photo, folk art

AI

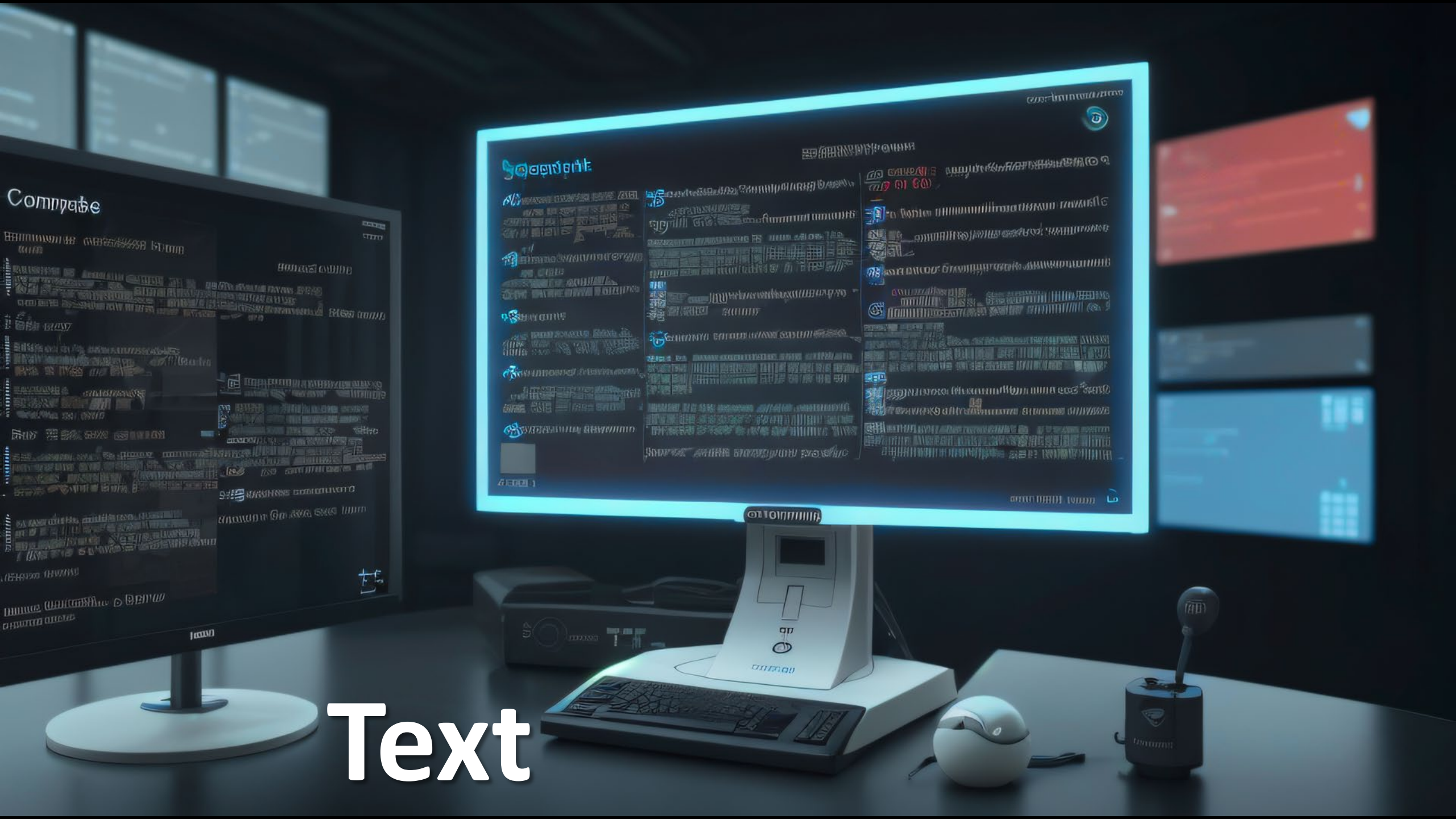
You keep using that word

**I do not think it means what you
think it means.**

Please talk about
Machine Learning
(because that's usually what it is)



ML Tools:



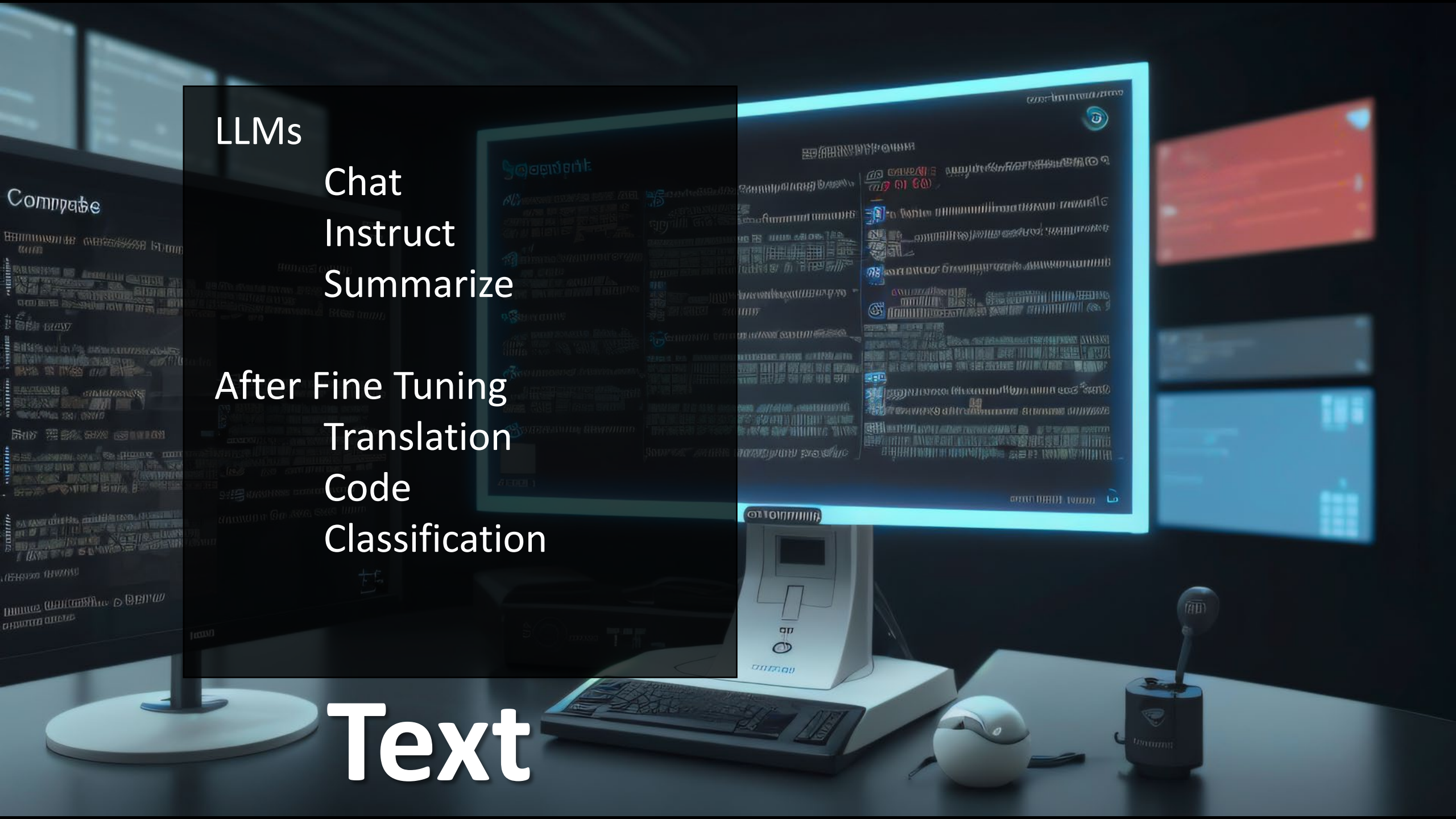
Text

LLMs

Chat
Instruct
Summarize

After Fine Tuning
Translation
Code
Classification

Text



LLMs

Chat

Instruct

Summarize

After Fine Tuning

Translation

Code

Classification

Good for Research

Audio



Audio

A professional recording studio with a mixing console, multiple monitors, and large speakers. The room is dimly lit with blue and green ambient lighting. The ceiling is covered in acoustic panels. The walls are lined with racks of audio equipment. A large monitor in the center displays a digital audio workstation interface with a waveform and various controls. The mixing console in the foreground is filled with numerous sliders and buttons. Large studio monitors are positioned around the room for monitoring audio.

STT

Transcription
Interactivity

TTS

Narration
Voice Cloning

Music

Experimental

Good for research

STT

Transcription

Interactivity

TTS

Narration

Voice Cloning

Music

Experimental



Images

Generative
Upscale/Enhancement

Segmentation
Identification
Classification



Image

Generative

Upscale/Enhancement

Segmentation

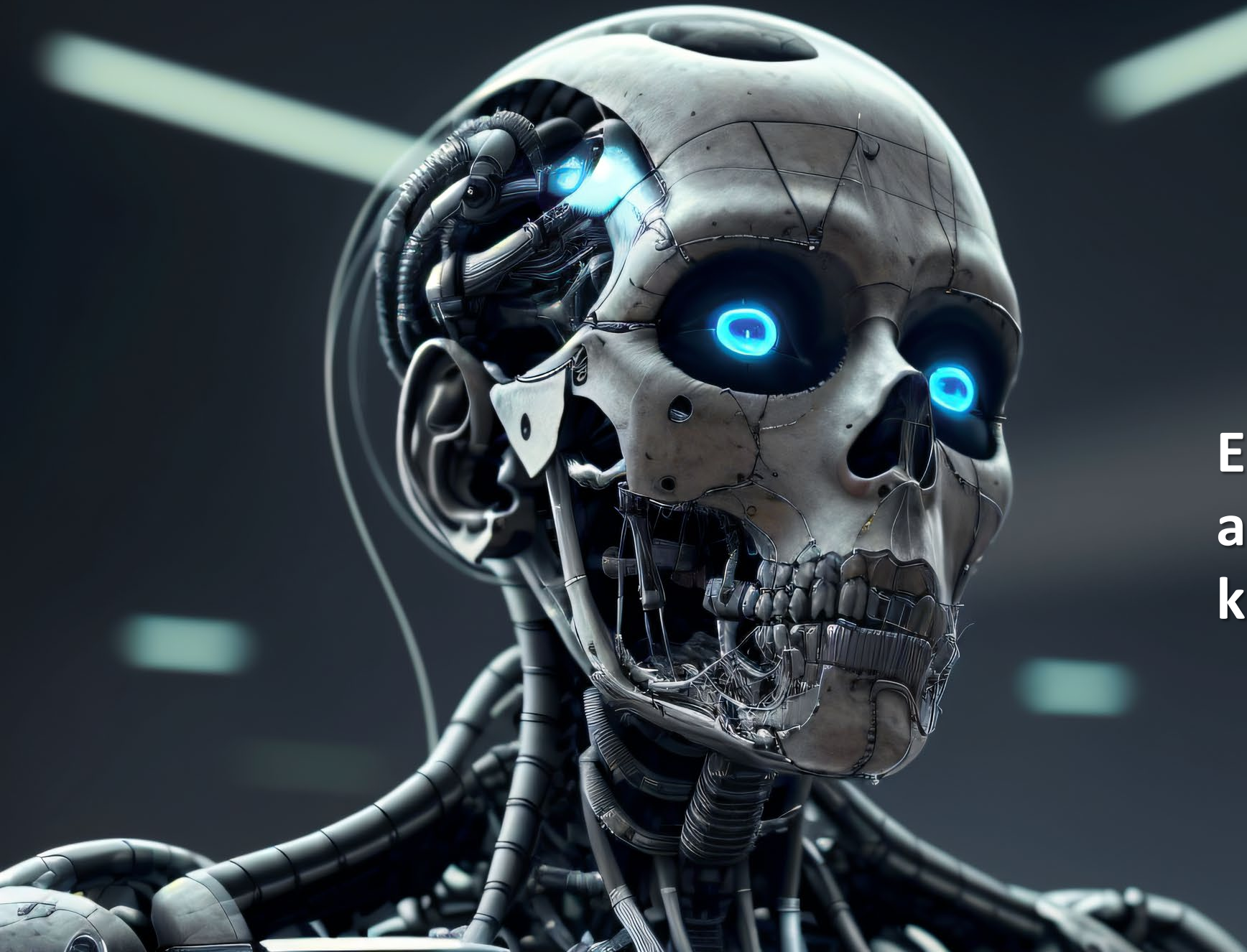
Identification

Classification



Good for research

Let's talk about risk...



Extensional risk,
artificial intelligence,
kill all humans, skynet

“Computers can, in theory, emulate human intelligence, and exceed it. Success in creating effective AI, could be the biggest event in the history of our civilization. Or the worst. We just don't know. So we cannot know if we will be infinitely helped by AI, or ignored by it and side-lined, or conceivably destroyed by it.”

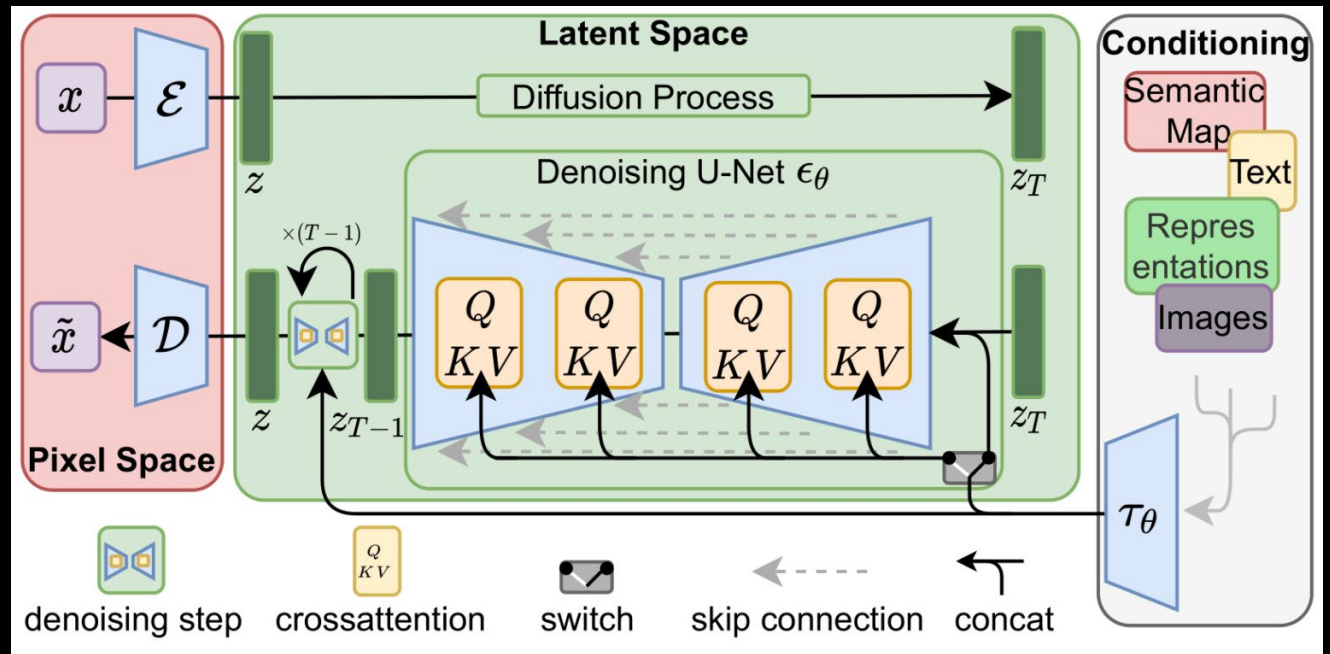
“While AI has the potential to transform society <...> it also comes with huge risks.”



- Stephen Hawking (2016)



This is NOT AI



https://en.wikipedia.org/wiki/Euler_method

Published: 1768–1770

This is AI

(ironically nothing on this slide was AI generated)

Steps: 40, Sampler: DPM++
3M SDE Karras, CFG scale: 7

Random Seed



883815727
+ 1

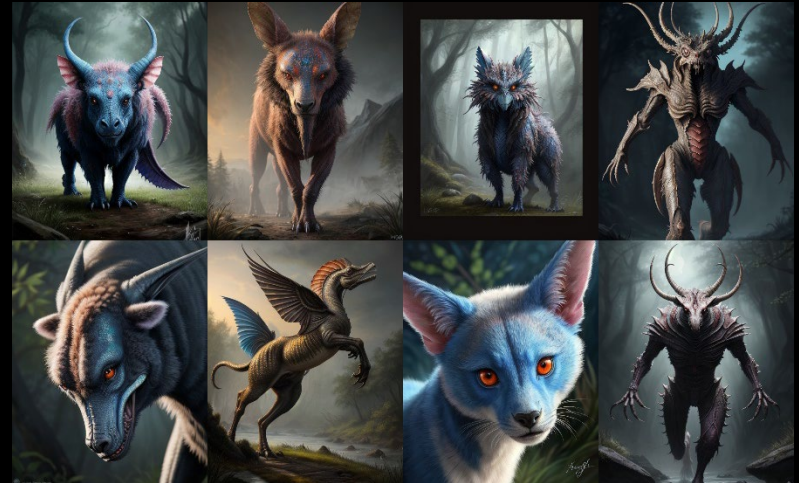
Math

+

Conditioning
(prompt)

a beautiful painting of
a creature, 8K, HDR

Output



This is AI

ML networks generate output based on statistical probabilities defined in a model.

There is no intelligence involved.

These networks do not “Hallucinate”, but frequently produce incorrect output.

This is AI

ML:

Related Risks (today)

Incorrect Information
Identity Fakes (Textual, Visual, and Audible)
Insecure Computer Code
PI and IP Leakage
Re-Identification
Polymorphic Malware
Poisoned ML Models
Knowledge Gap

<https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-use-generative-ai.html>



ML:

Ethical issues

Training data sources

Bias

Mental health

Knowledge Gap

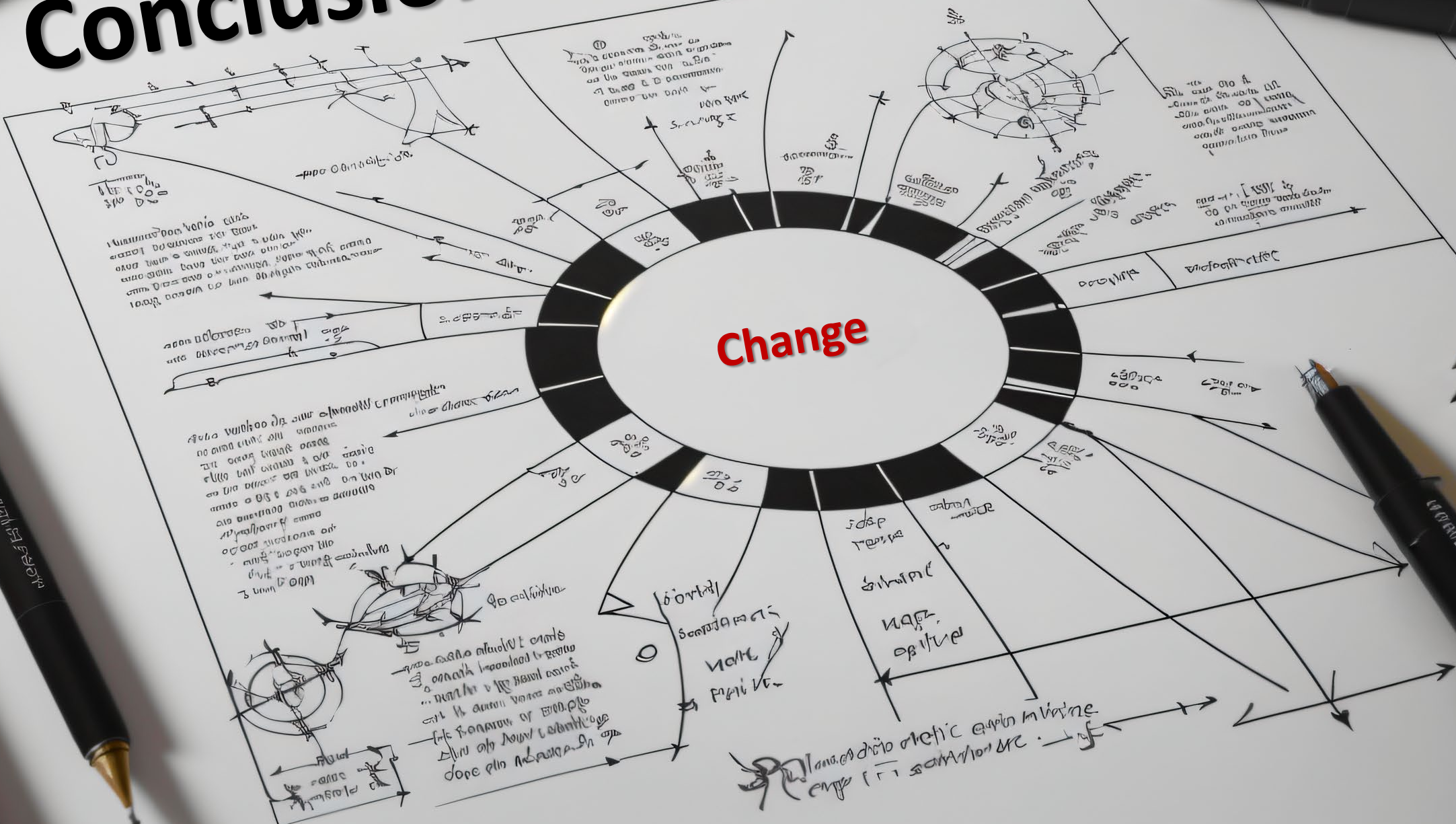
Environmental

Interference

Economic



Conclusions?



Conclusions?

Try not to anthropomorphize
Be careful with terminology
Never blindly trust a computer program
ChatGPT, Midjourney, etc... are like tiny grains of sand in
the expansive AI universe

Expect much more change & continue to adapt
Experiment – but use common sense
Engage in the ethical conversations

Current State of Research Information Security

It's a lot to unpack actually...



Termonology is problematic



Research Security != Research Information Security

Research Security

Foreign Interference

Infiltration

Partner companies

Academic fronts

Conferences

Coming Soon 2 Lists:

Entities

Sensitive Research Areas

Research Information Security

The background of the slide is a dark, blue-tinted image of a server room. Three individuals wearing black hooded sweatshirts are seated at desks, each working on a computer. The room is filled with rows of computer monitors and server racks, creating a sense of a high-tech, secure environment. The lighting is dim, with the primary light source being the screens of the computers and the ambient light from the server racks.

Phishing
Malware/Ransomware
Oversharing
Identity Theft
Exfiltration
Insider Threats
Unpatched/Compromised Systems

The existing threats are still here... just worse

Research Information Security

Phishing
Malware/Ransomware
Oversharing
Identity Theft
Exfiltration
Insider Threats
Unpatched/Compromised Systems

The existing threats are still here... just worse

But wait... there's more!

AI Generated Content
Cloud-sprawl
QR Codes

New Compliance Tools

Research Security:

Research Security Risk Assessments
Government Lists

Research Information Security:

Security Threat Risk Assessment
System Security Plans

CCCS + CSIS reaching out
Data Management Plans



Questions?

I have so many...

Next up...

Plugging security holes





Always follow institutional
policies & procedures

I say this because it is actually better;
...and also in fear of legal reprisals.



Security is like an onion...


It's got layers


Resources

- Brave Browser: <https://brave.com/>
- KeePass Password Safe: <https://keepass.info/download.html>
- Bitwarden Password Vault: <https://bitwarden.com/>
- Cryptomator: <https://cryptomator.org/>
- Interpol: <https://www.nomoreransom.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.

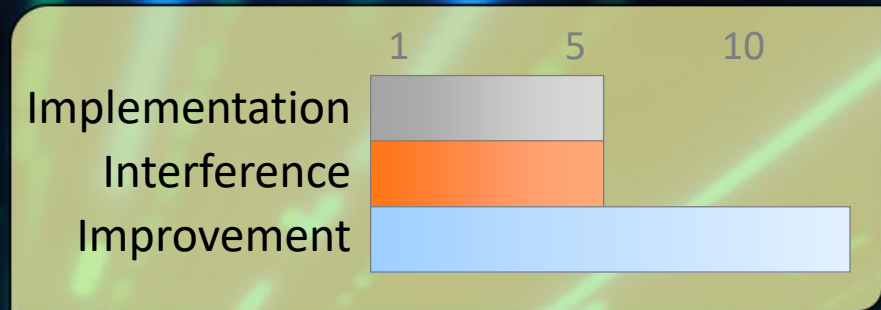
 Remember how to build passwords or generate them rather than trying to memorize passwords

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 > 15


Depending on the breach, different information is included.


Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the IPeassword password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

- Adobe:** In October 2013, 153 million Adobe accounts were breached with each containing an Internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and many were quickly reversed back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.
Compromised data: Email addresses, Password hints, Passwords, Usernames
- Avet Public Combo List:** In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Avet Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various other systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.
Compromised data: Email addresses, Passwords
- bittly:** In May 2016, the link management company Bittly announced they'd suffered a data breach. The breach contained over 5.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a small number using bcrypt.
Compromised data: Email addresses, Passwords, Usernames
- LinkedIn:** In May 2016, LinkedIn had 264 million email addresses and passwords exposed. Originally leaked in 2012, the data remained out of sight until being offered for sale on a dark market site 8 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.
Compromised data: Email addresses, Passwords
- MyFitnessPal:** In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2018, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HWP by a source who requested it be attributed to "berjandblue@exploit.in".
Compromised data: Email addresses, IP addresses, Passwords, Usernames
- MySpace:** In approximately 2008, MySpace suffered a data breach that exposed almost 350 million accounts. In May 2016 the data was offered up for sale on the "Real Deal" dark market website and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowercase and stored without a salt. The exact breach date is unknown, but analysis of the data suggests it was 8 years before being made public.
Compromised data: Email addresses, Passwords, Usernames
- Nexus Mods:** In December 2015, the game modding site Nexus Mods released a statement notifying users that they had been hacked. They subsequently closed the hack as being occurred in July 2013 although there is evidence to suggest the data was being traded months in advance of that. The breach contained usernames, email addresses and passwords stored as a salted hashes.
Compromised data: Email addresses, Passwords, Usernames
- QuintStreet:** In approximately late 2015, the maker of "performance marketing products" QuintStreet had a number of their online assets compromised. The attack breached 28 separate sites, predominantly technology forums such as Stack.com, codeguru.com and webdevelopment.com (later a full list of sites). QuintStreet advised that impacted users have been notified and passwords reset. The data contained details on over 4.6 million people and included email addresses, dates of birth and related MD5 hashes.
Compromised data: Dates of birth, Email addresses, IP addresses, Passwords, Usernames, Website activity
- River City Media Span Ltd:** In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain about 2.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an anonymous open operation. Once de-duplicated, there were 383 million unique email addresses within the exposed data.
Compromised data: Email addresses, IP addresses, Names, Physical addresses
- YSL4GURL:** In December 2015, the instant messaging application Yikraz.com suffered a data breach. The breach became known in July 2016 and exposed without personal data attributes including names, email addresses and passwords stored as salted MD5 hashes.
Compromised data: Dates of birth, Email addresses, IP addresses, Names, Passwords, Usernames
- tumblr:** In early 2013, tumblr suffered a data breach which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.
Compromised data: Email addresses, Passwords
- Verifications.ie:** In February 2018, the email address validation service verifications.ie suffered a data breach. Discovered by Bob Dickhardt and Henry Trost, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and reached in 700 million unique email addresses before exposure. Many records within the data also included additional personal attributes such as name, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.ie website went offline during the disclosure process, although an archived copy remains searchable.
Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

Unique Passwords (Secrets)

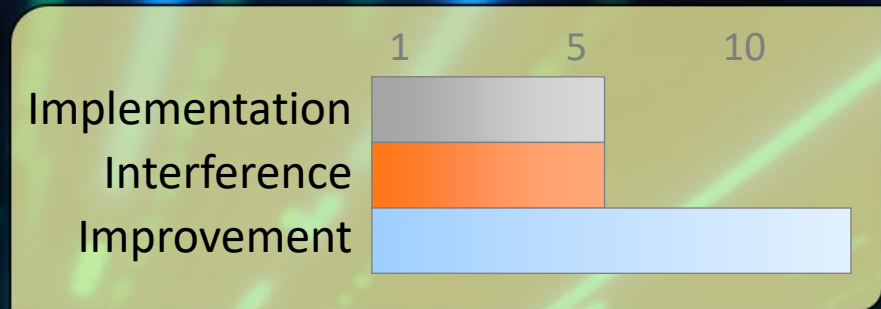
 The single most important good habit:
Prevent one site's breach from exposing all your accounts.

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

Size matters – use passphrases – not guessable


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.

Use a Password Vault

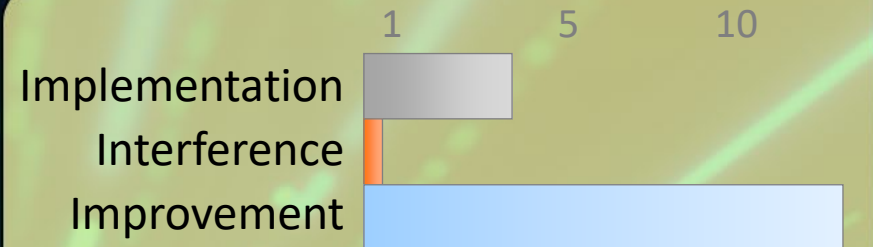
 Single encrypted location to store and manage secrets.

 Generate your passwords for you

Store other kinds of secrets


Securely send information to others


Is actually faster... really!



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

Use Multi-Factor Authentication

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

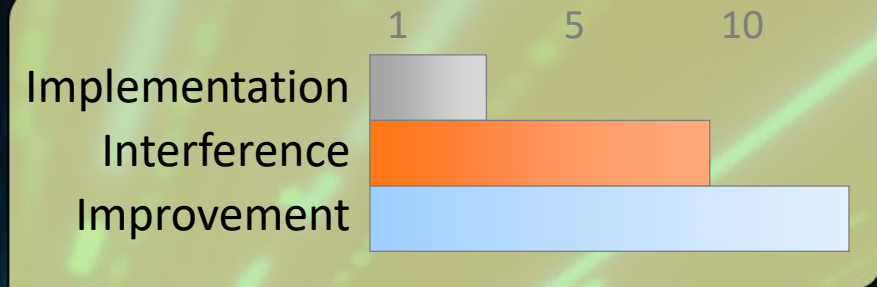
 Something you Have, Know, or Are

SMS is insecure, but still better than nothing

Many options exist, many systems support it.

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


Beware MFA - Fatigue




Bonus Tip:

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

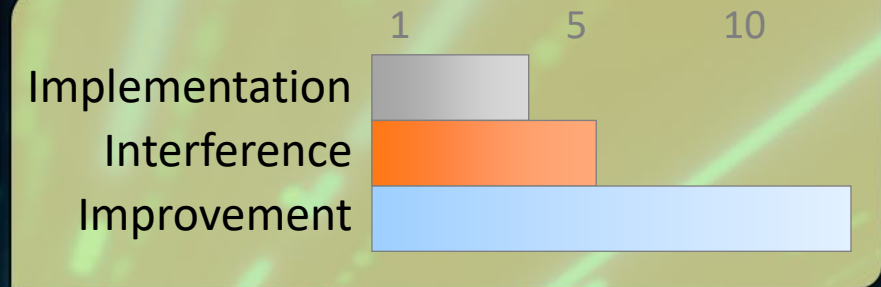
Security Questions & Answers

 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.

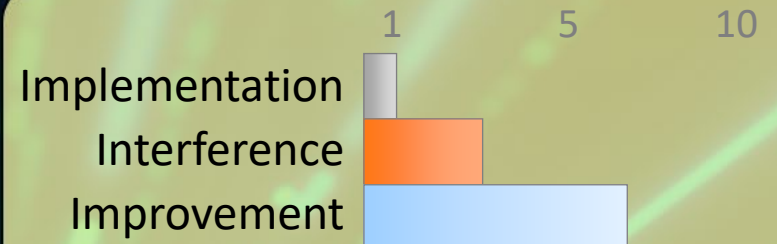
Browser Memorized Secrets

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

 Leverage a password vault that keeps your secrets safe.

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.

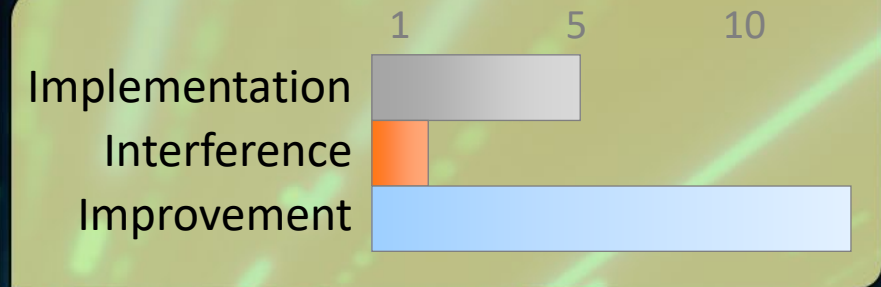
Protect any Recovery/Reset Pathways

 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.


Consider establishing different recovery information for different accounts.



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

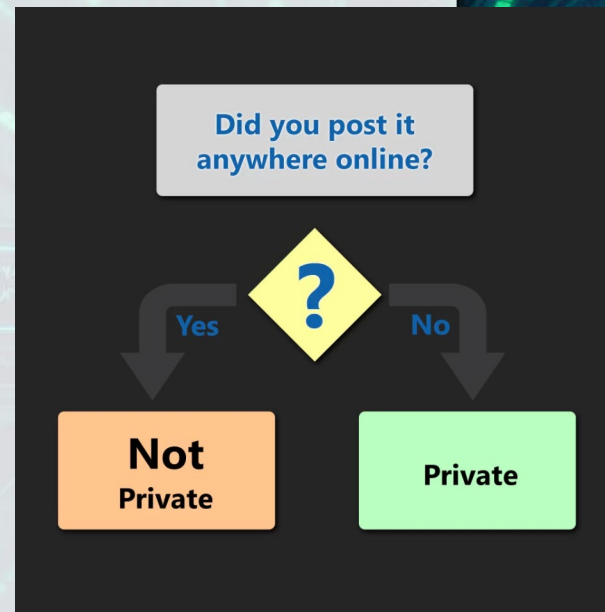
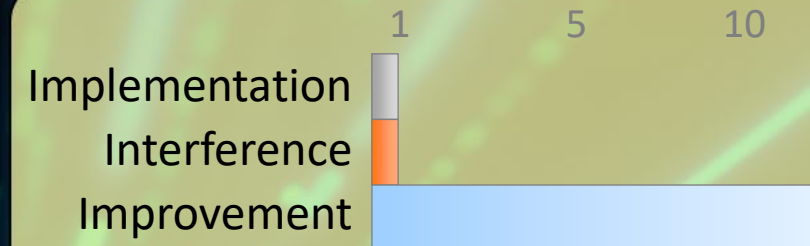
Social Sharing and Privacy

 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.

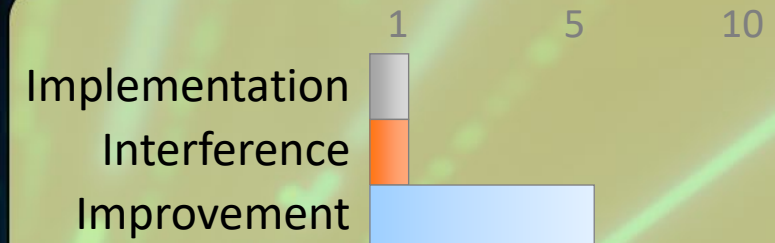
🎯 Think before you scan that QR code

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

💬 Check for stickers over the real code.

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 add to the URL.

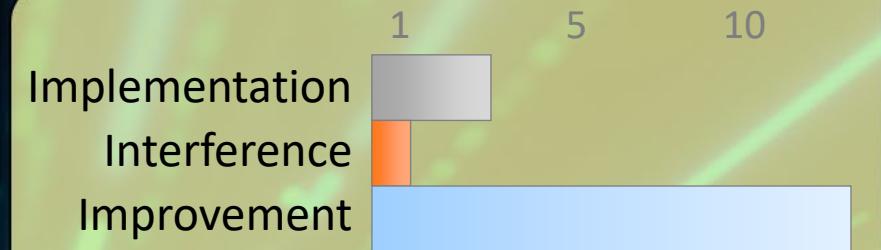
Delete Unnecessary Information

 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.

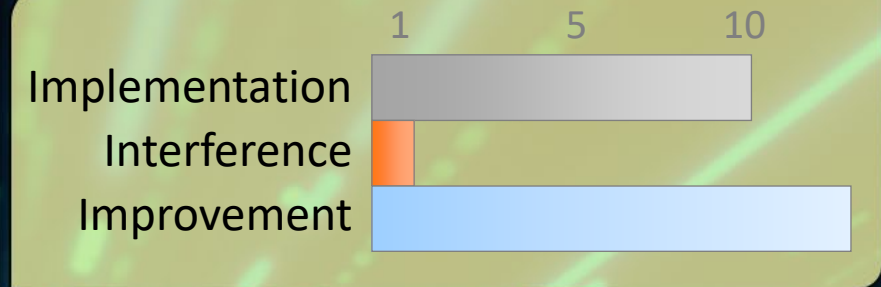
Have Backups and Plan to Restore

 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.

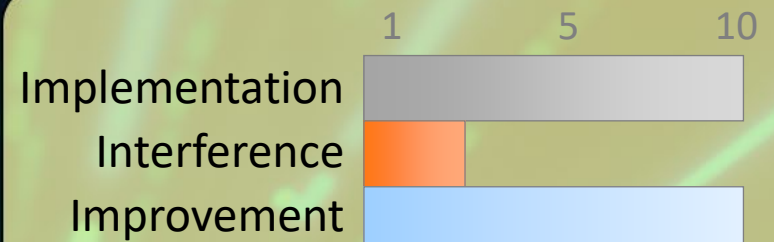
Use a VPN

 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.

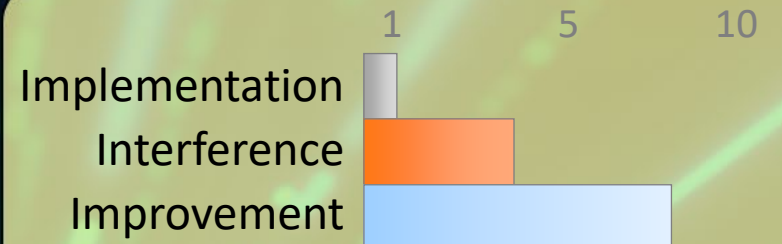
Don't Blindly Copy and Paste Code

 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 Tactics

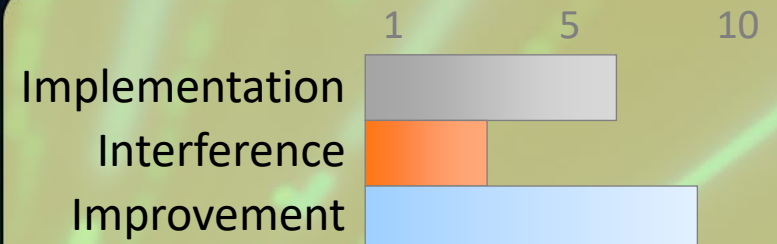
Audit Authorized Apps

 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.

Reset Default Passwords

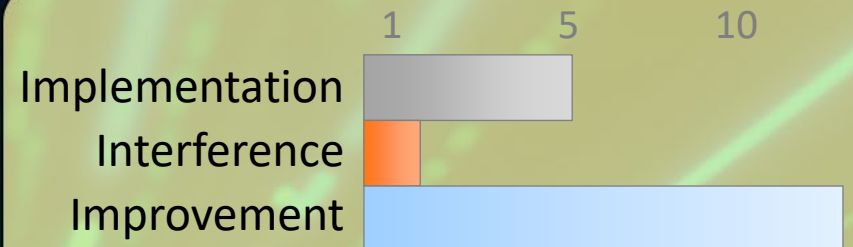
 Mitigates bots / scripted compromise
Easier for you to access

 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!

Apply Software Updates

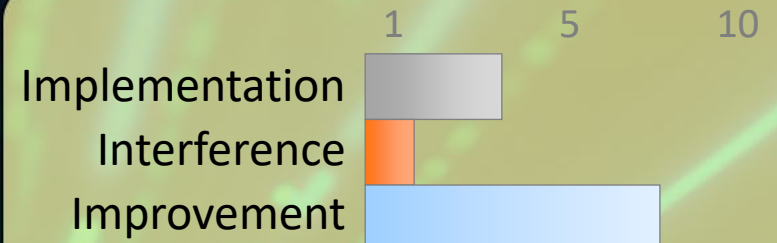
 Smart people are working hard to fix vulnerabilities: Take advantage of that (usually free) protection.

 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! (UBC: Weekly at a minimum)




Bonus Tip:

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

Supply Chain Trust

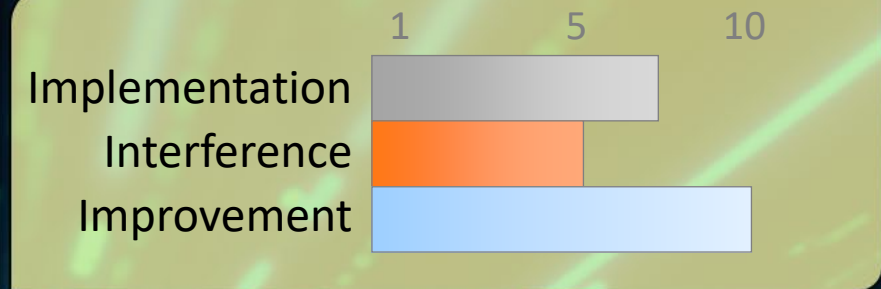
 We must know what is in the software, to trust it.

 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.

Sometimes custom written code is actually faster and more efficient.

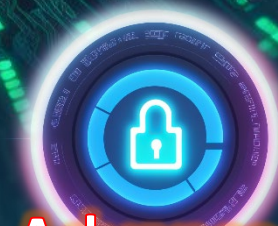
Check/Maintain a Software Bill of Materials (SBoM)



Bonus Tip:

Diff library updates to review changes.


Implement scanners for known injections.



Advanced Tactics

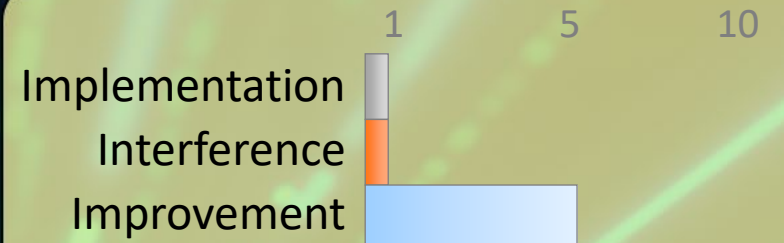
Show File Extensions

 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.

Authenticate to Unlock

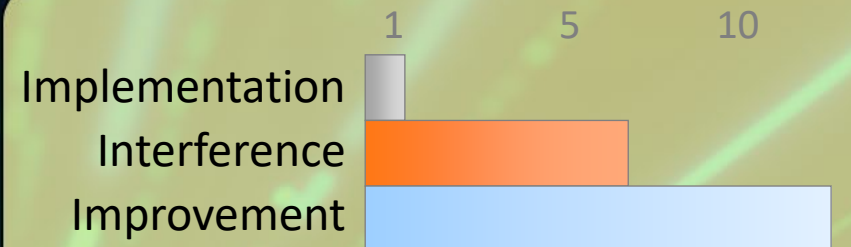
 An unlocked device in the wrong hands has full access to everything you normally do.

 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.

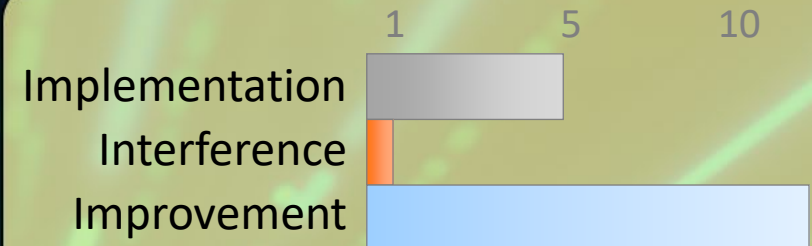
Identity Theft

 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.

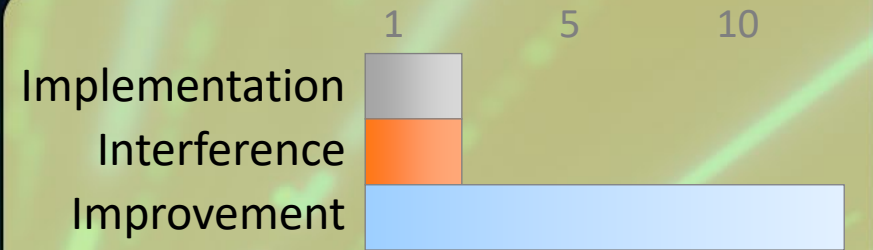
Power Off

 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.



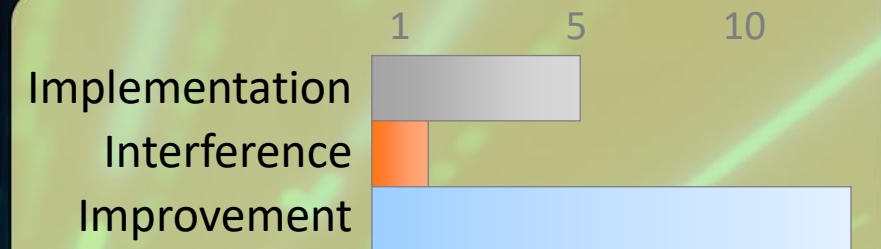
Bonus Tip:
This will also save you money in electricity charges.

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.

Keep Recovery Information Secure

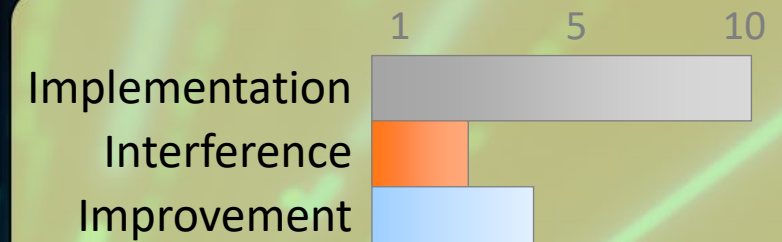
 This can be the weakest link in the chain, the password is useless If someone can reset or recover it.

 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 and the information you provided for all 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.

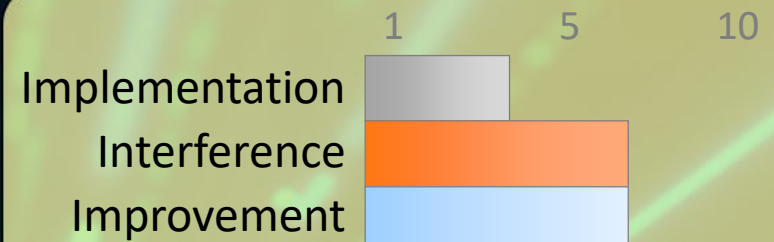
Do not use "found" or "free" USB keys unless you trust them.

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.

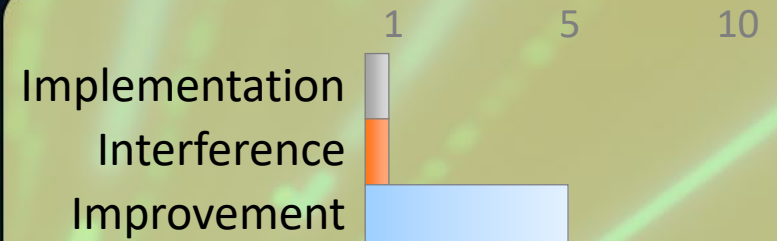
Be wary of USB charging stations

? 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 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:

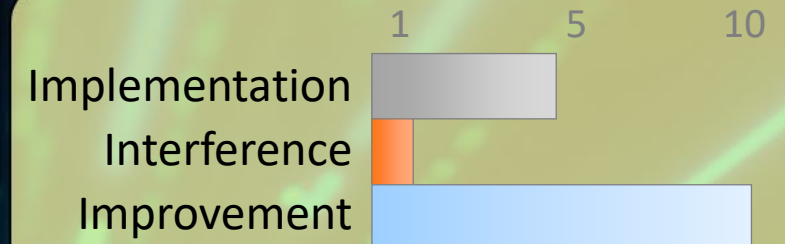
Cars with USB ports can capture a lot of your personal information if you connect – read the privacy policy!

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:

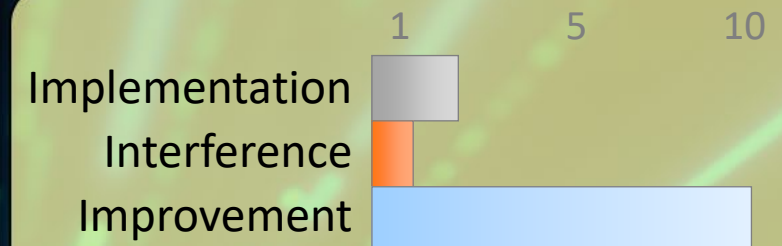
The encryption key (or recovery code when applicable) must be very carefully secured.

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.



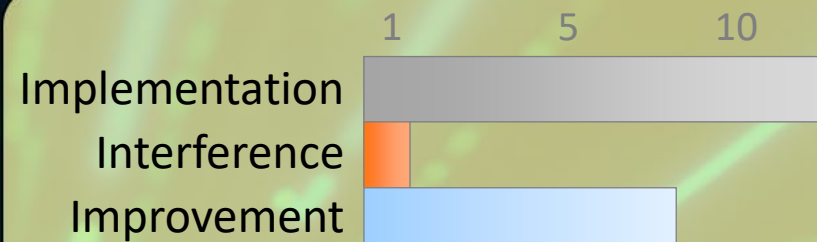
Bonus Tip:
Laptop screen
privacy filters (\$30)
provide extra
protection in busy
locations

Segment your IOT devices

 A more restricted 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 Tactics

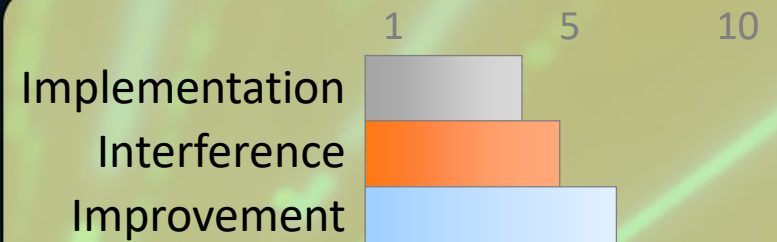
Photo Sharing – Hidden Data

 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 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.

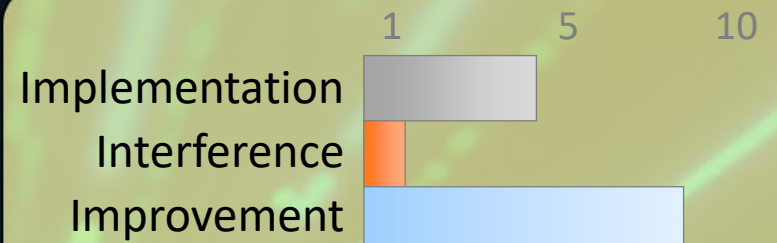
Audit Shared Folders

 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 no longer required.




Bonus Tip:

This can save space on your hard drive as well.

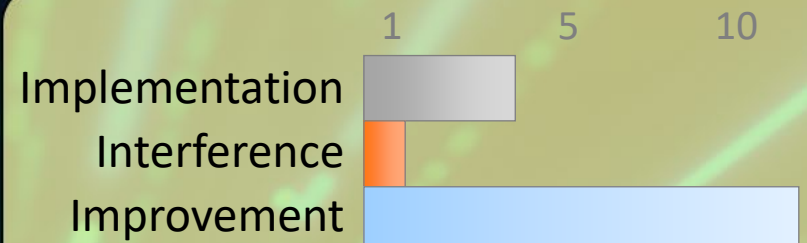
Sanitize before Disposal

 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.

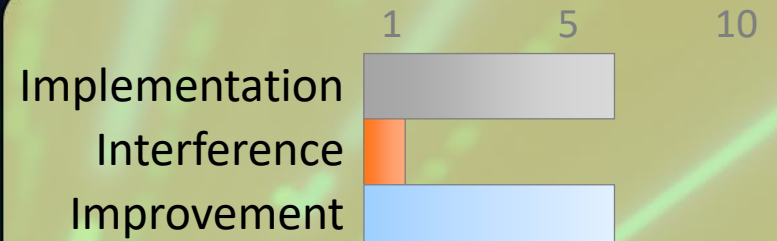
Securely Delete Files (Cloud)

 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.

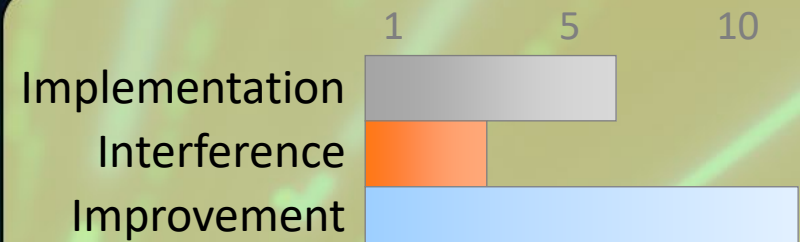
Use Encryption (cloud/file)

 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/>



Bonus Tip:

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

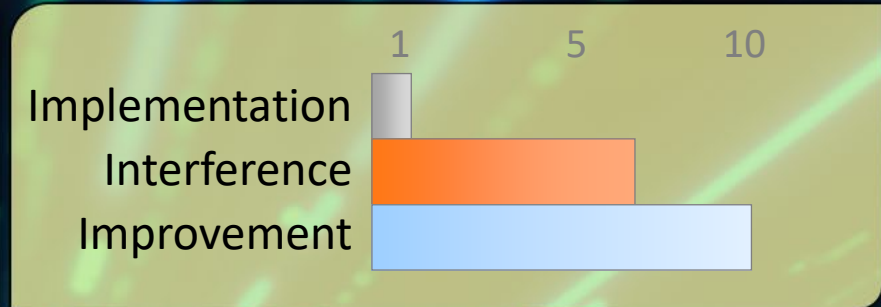
🎯 Enable Quick Auto-Lock

❓ 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 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!

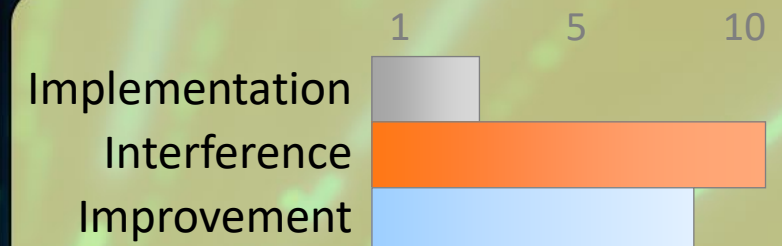
Sign-out

 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:

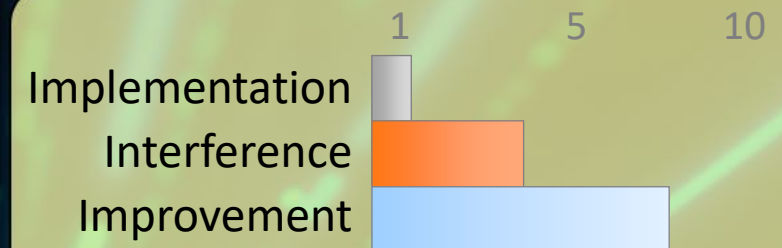
Wiping cookies will sign you out of most services in a single step.

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.


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!

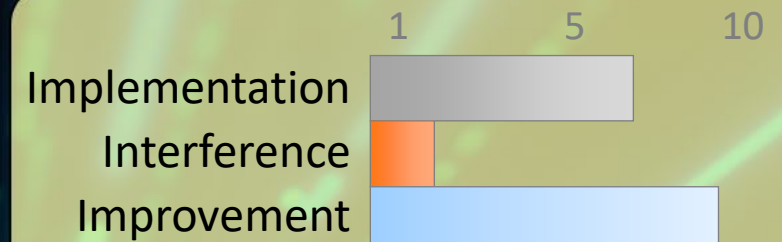
Guest infection through WiFi

 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 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.

Block Ads, Flash, Trackers

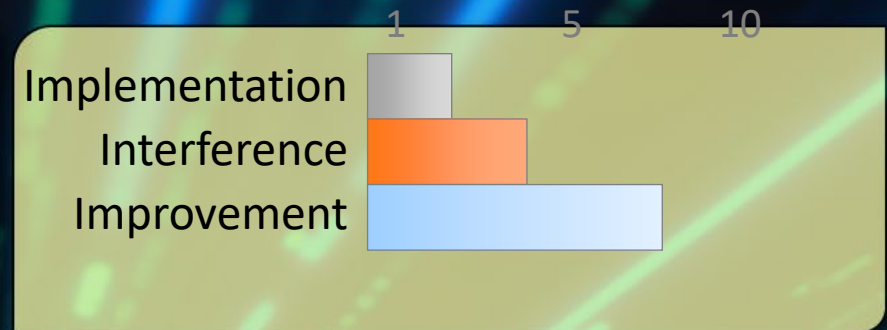
 Flash is riddled with security holes, ads frequently serve malware and you likely don't want them anyway.

 Getting old – but still useful advice.

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.



Let's keep in touch

email: scott.baker@ubc.ca

blog: <https://scottbaker.ca/>

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

