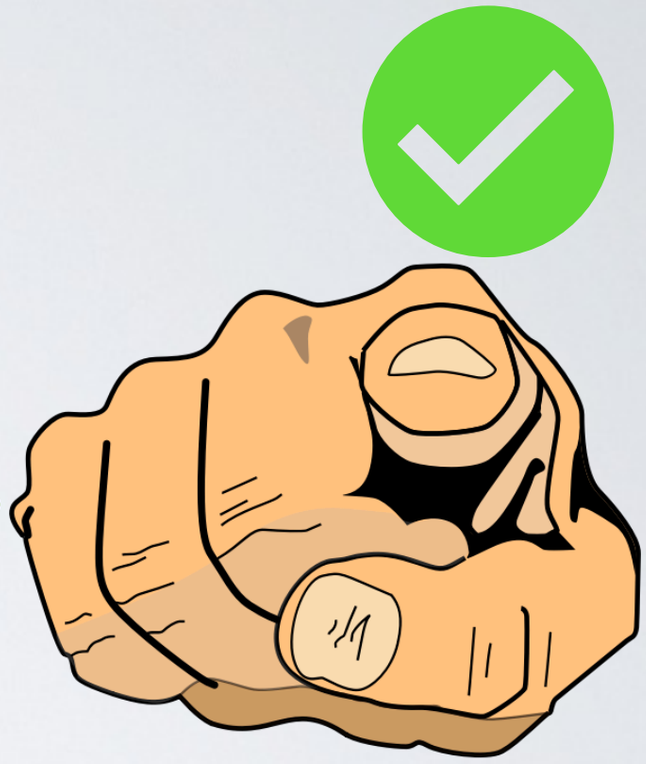
Human Security

Kc Udonsi

VS



Threats humans face in cyberspace

- Credential theft
- Identity/PII theft, Impersonation, Account takeover
- Cyber bullying, extortion, stalking
- Online scams e.g moving, job hunt, cheque, delivery etc
- Digital bank fraud, etc

How can we mitigate these ? …

➡ **Properly managed personal digital assets and technology (Good cyber-hygiene)**

- Use of trusted and secured networks
- Securely update any networked device's default configurations
- Keep software and devices OS and firmware up to date
- Be suspicious of and verify all electronic information requesting urgent action

How can we mitigate these contd ? …

➡ **Properly managed personal digital assets and technology (Good cyber-hygiene)**

- Share responsibly (incl. shared devices)
- Good password hygiene
- Verify and validate all software prior to installation
- Use reputable EDR solutions
- Proper data lifecycle management

How can we mitigate these contd ? …

➡ **Properly managed personal digital assets and technology (Good cyber-hygiene)**

- Good physical security for devices and secure facilities
- Reporting suspicious or malicious physical or cyber activities to appropriate personnels

➡ **Security awareness and training**

Trusted and Secure Networks

Wifi, VPNs, TLS

Good Network Security Hygiene

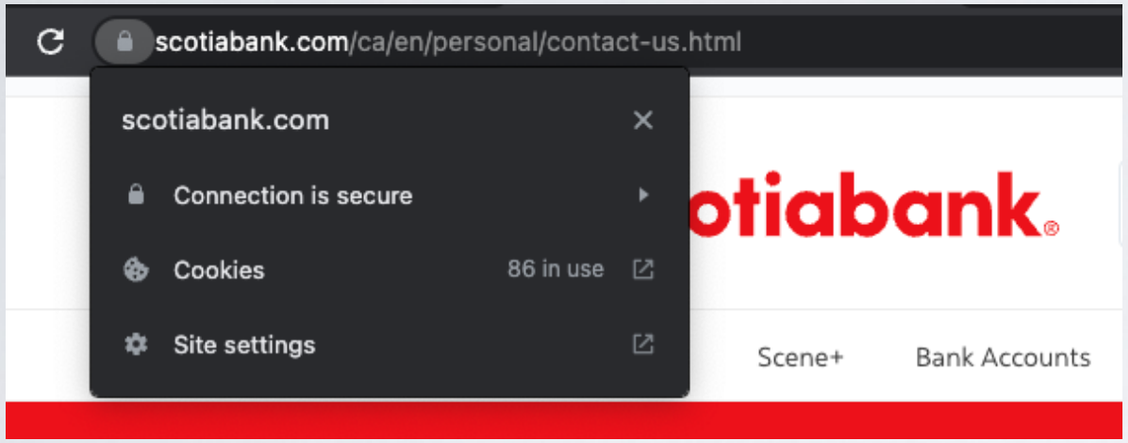
➡ **HTTPS Everywhere**

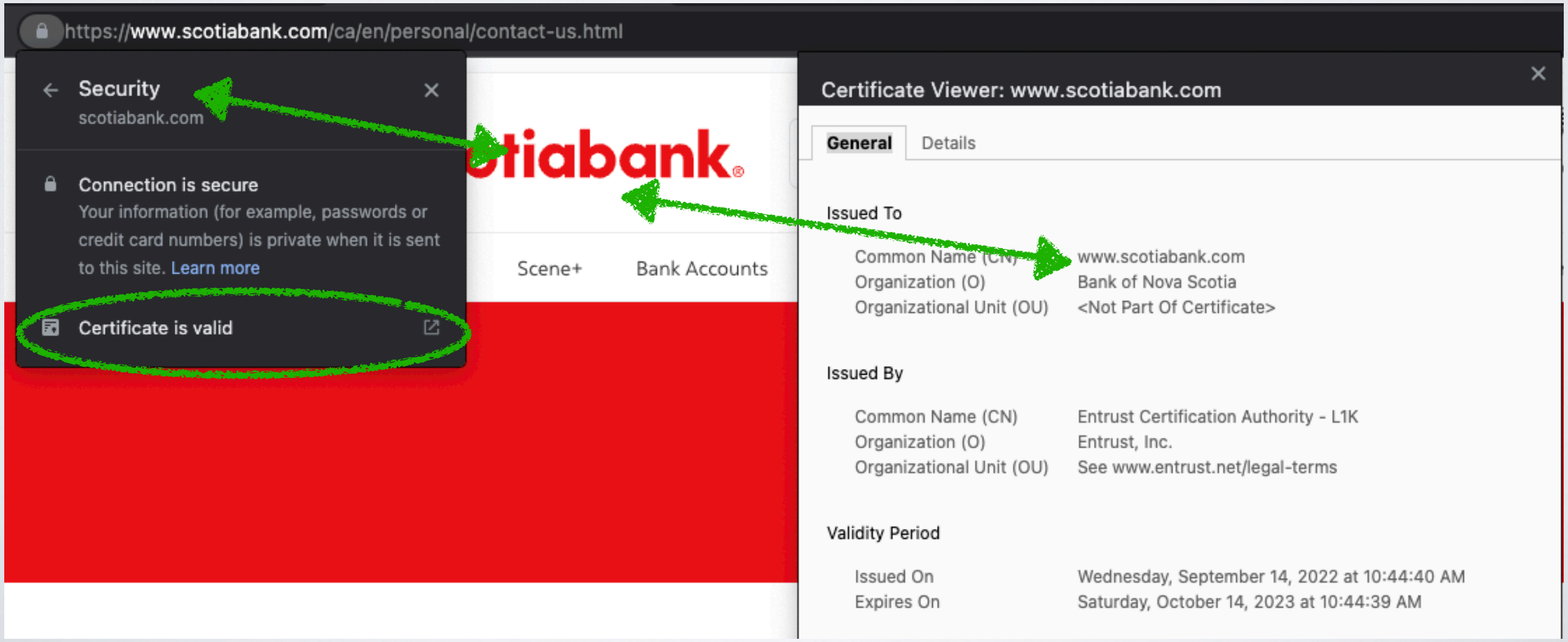
- Ensures that information you share with trusted applications remains confidential even on untrusted networks

- Verify the URL and ownership of any sites requesting information or soliciting actions e.g ***Support call #s***, ***chat-bots***, ***credentials*** and ***other Personal Identifiable Information***

- Not sure about a site's legitimacy? Investigate securely using platforms like: urlscan.io

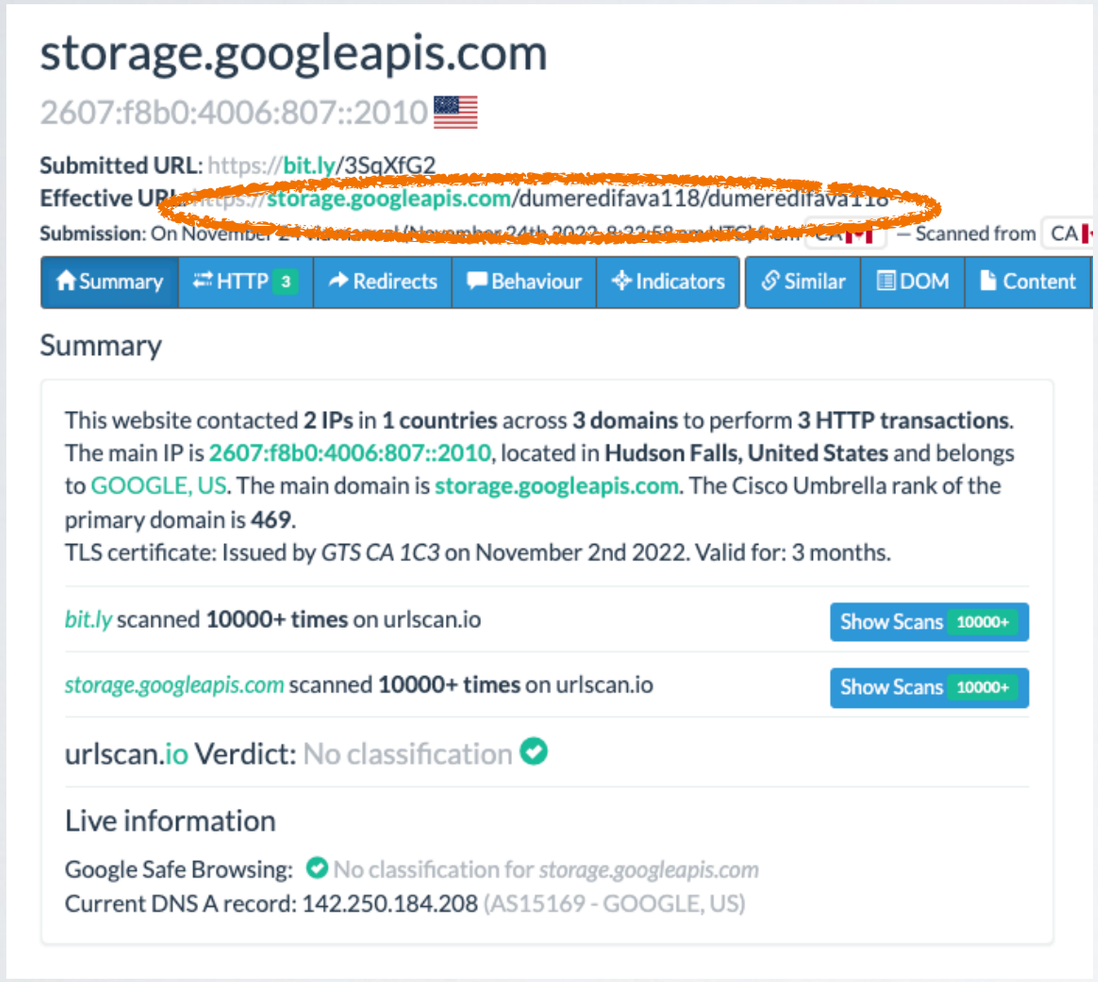
Good Network Security Hygiene - HTTPS

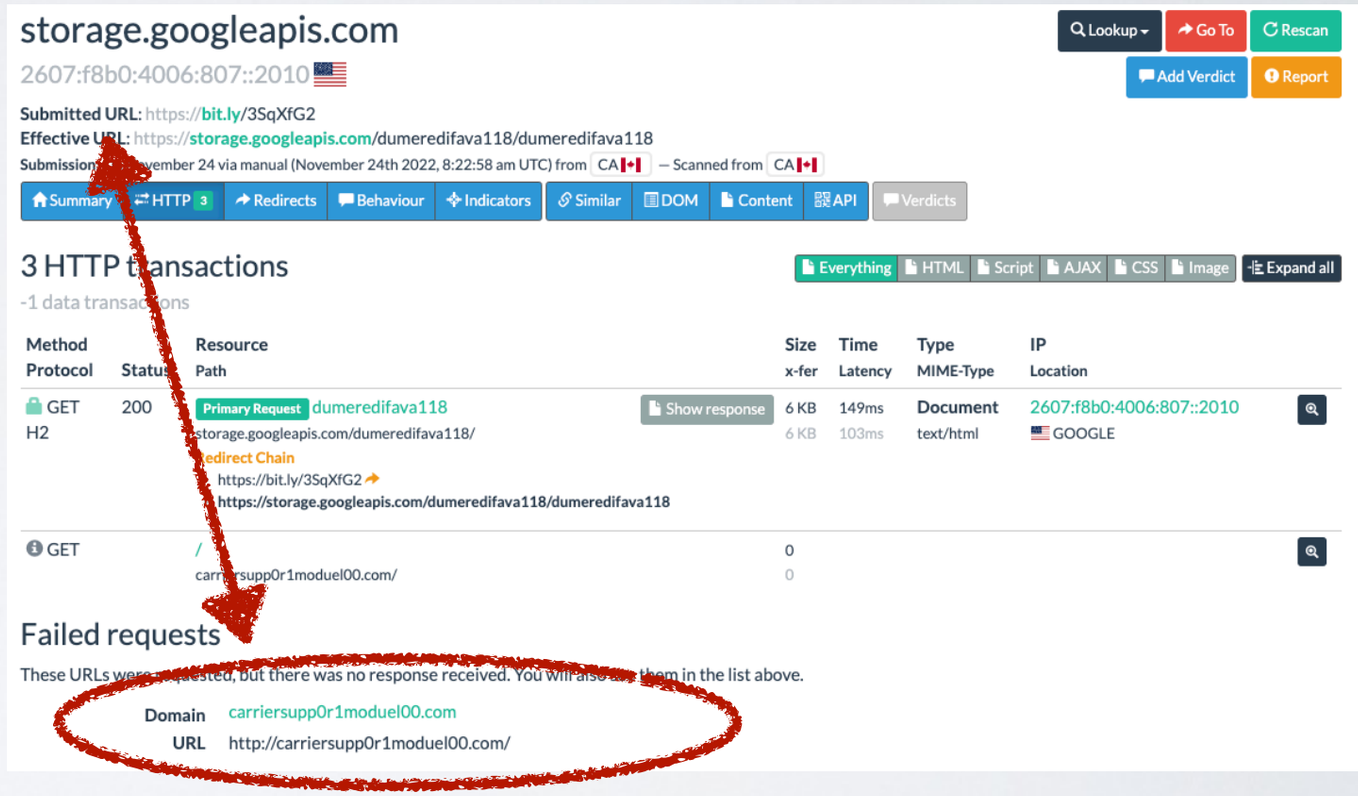




Good Network Hygiene

➡ Is this URL malicious?





➡ YES!

Good Network Hygiene

➡ **HTTPS Everywhere and Cert verification mitigates**

- Credential theft due to plain text transport

- Site impersonation. Don't naively trust it because it's GREEN! Both the certified domain and issuer must be trusted. "**If it looks like a duck but isn't certified as a duck, it is not a duck**"

Good Network Hygiene

➡ **Wifi & captive portals security**

- Secure WiFi ensures devices are connected to the appropriate access point and communication between AP and endpoint are encrypted
- Modern schemes include WPA2/3 Personal AES and Enterprise.
- Be wary of "Free", "Unsecured", "Weak Security" and potentially fake captive portals

Good Network Hygiene

➡ **Wifi & captive portals security**

- Bring Your Own Hotspot
- Use a secure tunnel or VPN to a trusted network
- Check device for Wifi warnings

➡ **Wifi & captive portals security mitigates**

- PII theft due to MITM

Secure devices and facilities

Latest updates, vulnerability and access management

Good Device and Physical Access Hygiene

➡ **Software Updates**

- Ensures that devices are running the most updated versions of software and firmware and thus are not vulnerable to ***known*** attacks

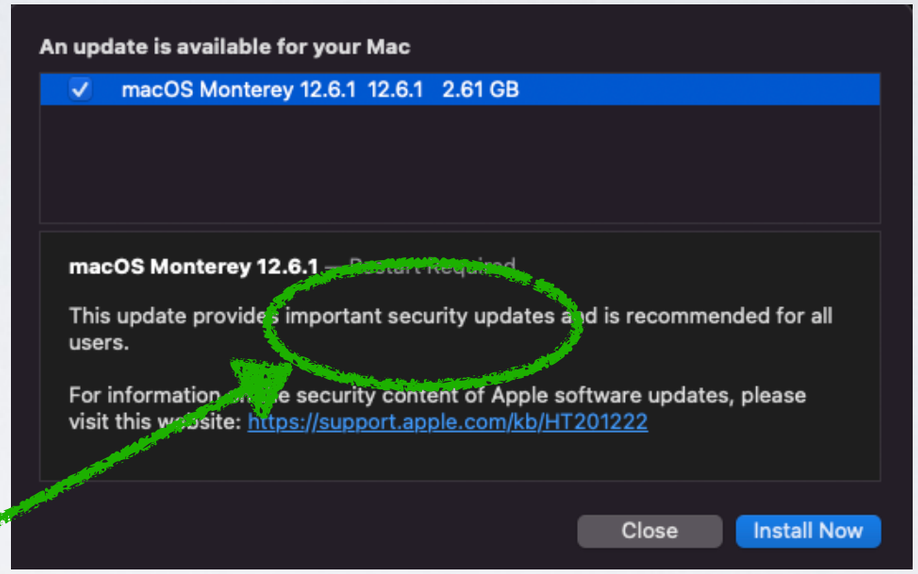
- Update software and OS versions as early as possible. Fixes may include patches for in-the-wild zero-days or actively exploited vulnerabilities

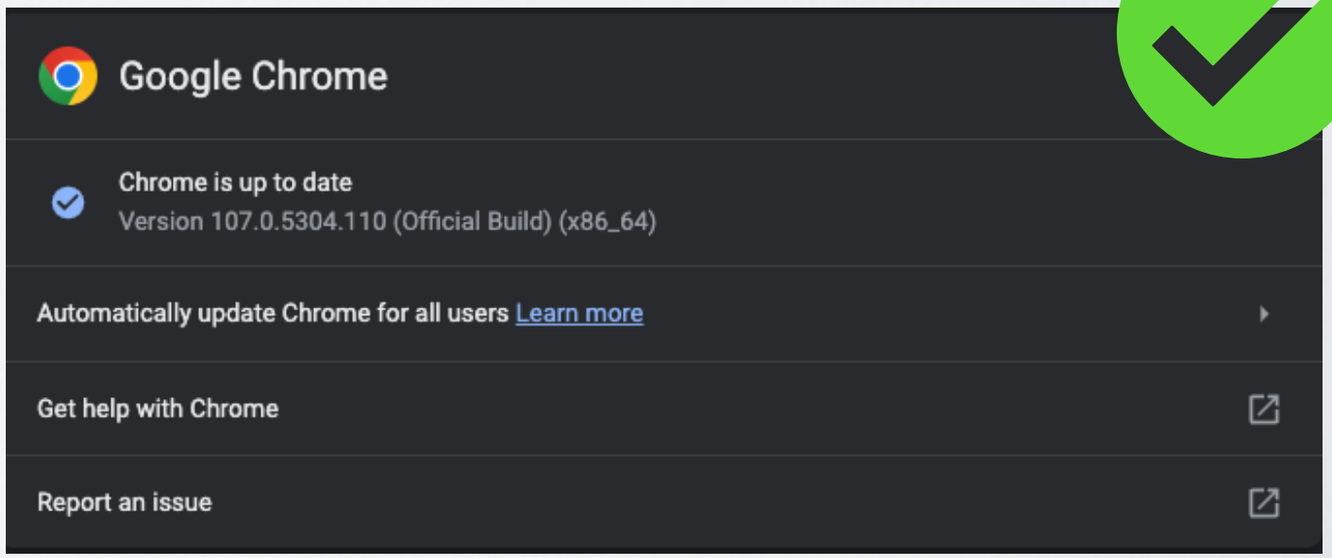
Good Device and Physical Access Hygiene

➡ **Use legitimate and verified/authorized software**

- Cracked or illegitimately downloaded software could very well be malware
- Verify downloads by confirming provided hash
- Thoroughly inspect download links to ensure the resource is hosted from the expected source
- *You may not have paid for that software with money but you probably paid with your personal security*

Good Device and Physical Access Hygiene





Good Device and Physical Access Hygiene

➡ **Device passwords/passcodes and biometrics**

- Prevents unauthorized access to a device
- Passcodes should be at least 6-digits and consider passphrase/passwords
- Do not rely on passwords and or biometrics by themselves consider ***multi-factor-authentication****
- Update any default router and IoT management portal and device credentials

https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

Good Device and Physical Access Hygiene

➡ **Privacy screen guards and Screen Lock**

- Limits viewing angles of personal devices. Protects sensitive information on display panels such as phones, tables, laptops etc

- Do not leave devices unlocked and unattended

Good Device and Physical Access Hygiene

➡ **Protect connectivity ports**

- Device ports like USB and network ports like Airdrop, Bluetooth must be protected or disabled where applicable
- Unpair and disconnect
- Do not plug-in unknown media drives or connect to unknown wireless sharing networks such as Airdrop, bluetooth etc.

Good Device and Physical Access Hygiene

➡ **Secure facilities access**

- Keycards and key fobs are often issued to authorized personnel for access and audit purposes

- DO NOT
  - Hold open secure doors
  - Swipe access cards for anyone other than yourself
- Be aware of tailgating, piggybacking, loitering etc

Good Device and Physical Access Hygiene

➡ **Good Device and Physical Access Hygiene mitigates**

- Physical data theft and installation of adversarial network components
- Device compromise via adversarial human-interactive-devices
- Software exploits

Secure online presence

Responsible sharing, password management, scam/fraud detection

Good Online Hygiene

➡ **User authentication**

- Online platforms need to authenticate and subsequently manage user access.
- Authentication can be performed by the following factors
  - *Something you know*
  - *Something you have*
  - *Something you are*
- Ideally these factors would be out of reach to threat actors

Good Online Hygiene

➡ **Good password security**

- Ensures unauthorized access to online accounts
- Create strong passwords
  - Use a secure password generator OR
  - Make it easy to remember hard to guess or brute force in reasonable time
- Do not reuse, share or store in plain-text. Consider password managers

Good Online Hygiene

Passwords Are Like Underwear

Cyber Security Top Tips

mtechsystems

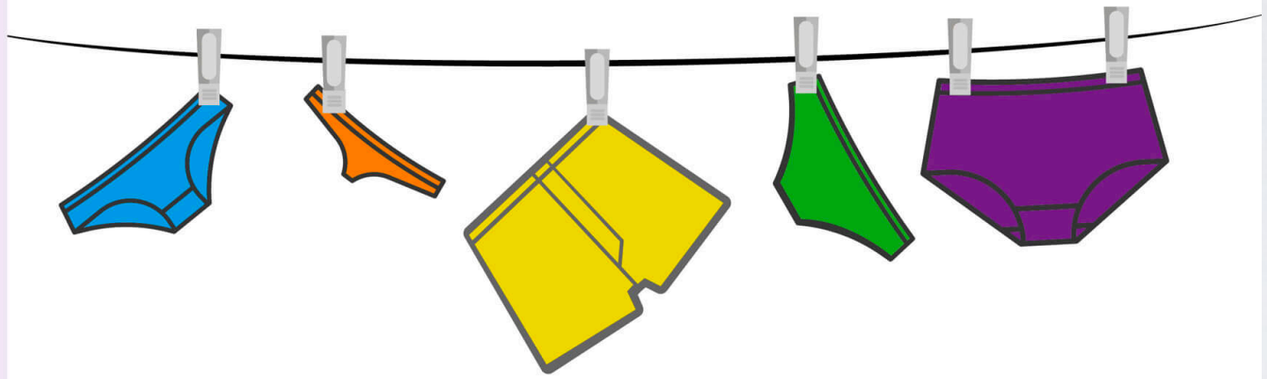
Proven Innovation

PASSWORDS

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data. Here are a few tips for looking after your passwords.

Don't pick a password that could be easy to guess e.g. a family or pet name

Don't use the same password for more than one login



Don't leave them lying around

Change them regularly

Don't share them with anyone

IT Services. IT Solutions. IT Support **t:** 01323 404040 **e:** info@mtechsystems.co.uk **www.mtechsystems.co.uk**

Good Online Hygiene

➡ **Good password security**

- Enable multi-factor authentication (MFA)
  - Combination of any of the factors of authentication. Often
    - *Something you know* + *Something you (are | have)*
  - Last line of defence against compromised credentials
- Build apps that support MFA
- Do not give/send MFA codes (often 6-digits) to ANYONE!

Good Online Hygiene

➡ **Secure online communication/interaction**

- Ensures web of trust is not abused for compromise and data theft
- Applies to all forms of non-physical communication: ***calls***, ***direct messages***, ***SMS***, ***email***, ***voice-messages*** etc
- Re-authenticate and verify sender whenever via out-of-band
  - An actionable or downloadable information is received
  - A request or prompt is made (incl. links)

Good Online Hygiene

➡ **Secure online communication/interaction**

- Be wary of electronic communication triggering heightened panic, fear, anger, joy, curiosity, urgency etc

- Avoid oversharing via text or images on social sites e.g containing personal spaces, device screenshots, secure facilities

  - Avoid volunteering information

- Be wary of spelling mistakes and when communication cannot be verified

Good Online Hygiene

➡ **Verifying an email sender**

- Emails can be exported/saved as ***.eml.*** This format can be opened safely in a text editor

➡ **Is that legit?**

- @mail.utoronto.ca?

Incident Reporting and Recovery

Credentials, Identity, PII, account takeover

A matter of personal safety …

➡ **Report (attempted) PII and data theft**

- Report to most applicable authority. Often sites or institutions such as banks, employers, social media have their report centres for cyber crime and fraud

➡ **Report cyber extortion, harassment and bullying**

- Report to local law enforcement, campus security

➡ **Change and update credentials**

- If you suspect a breach has occurred change credentials immediately

Security Awareness

Continuous training and evaluation


ONE CAN NOT
NAIVELY BE ONLINE
imgflip.com

Security Awareness

- See week10 resource section for links on staying safe online
- Regularly take trainings to keep abreast with adversarial tactics
- Share this knowledge with friends and family
  - The internet is hostile territory
  - The adversary has no regards for the victim status, age, nationality, life situation, mental health etc