V.A.Karthik, ACM/C&I
04-11-2025
karthik_va@nlcindia.in

Cybersecurity - Best Practices

Vigilance Awareness Week - 2025

सतर्कता: हमारी साझा जिम्मेदारी

Vigilance: Our Shared Responsibility

- Theme of VAW 2025

Agenda

- Passwords and Management
- DNS & DNS filtering
- Spam & Scam
  - How to Identify ?
  - How to protect ourselves ?
- Privacy & Digital Wellbeing

Passwords and Management

- How Are We Managing Our Passwords ?
- How many online accounts we have ?
- Are we re-using the same password ?

Password Statistics

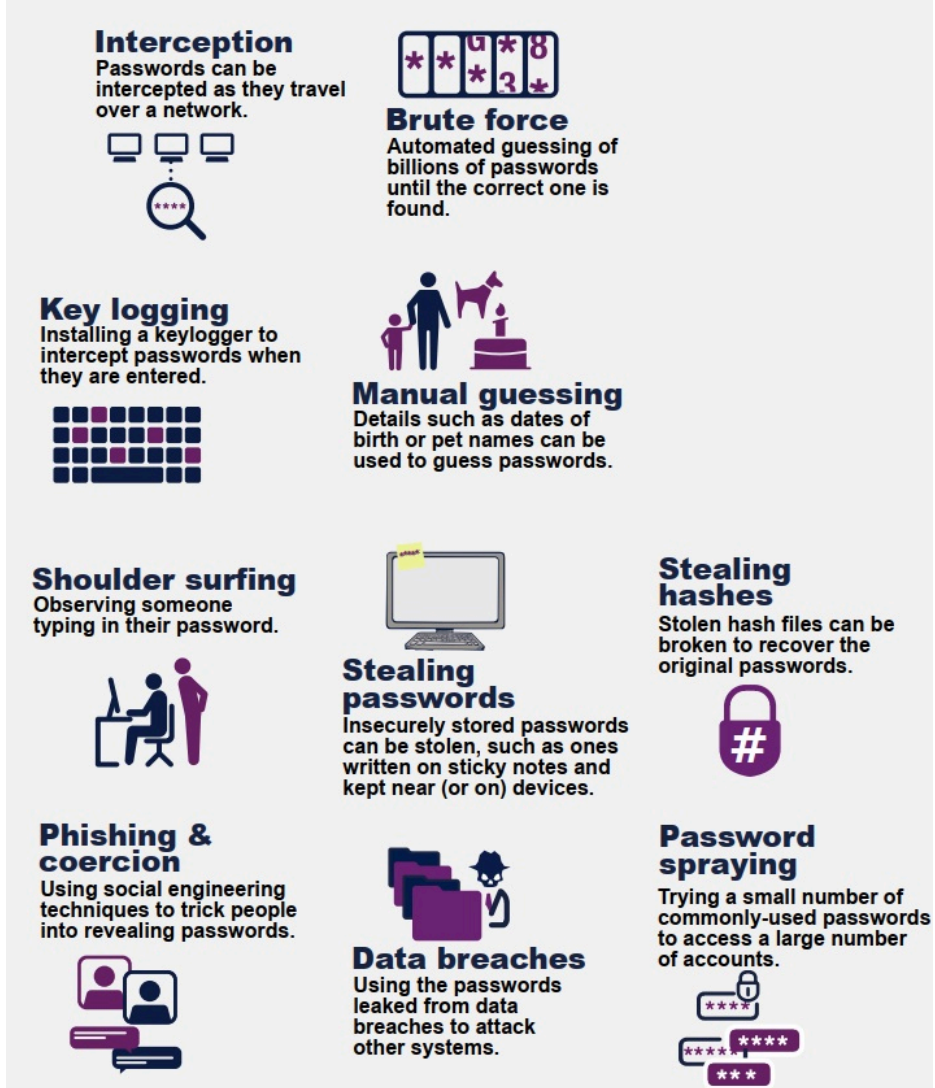
- "123456" still top-used globally (nordpass)
- Average person has **100+ accounts** (nordpass)
- 51% have their passwords memorized (security.org)
- On average, people reuse the same password for at least four accounts (forbes advisor)

Passwords and Management

→

How Passwords are Compromised

full infographic here



Have I Been Pawned ?

- Website: https://haveibeenpwned.com
- Run by security researcher **Troy Hunt**
- Database of compromised passwords
- Everyone is vulnerable to phishing - Troy Hunt's Mailing list leak example

Passwords and Management

Passwords and Management

Problem with Passwords

- Should be Unique for each website
- Impossible to remember
- Each Website Enforces different password policy and expiry

Password Managers

- Securely Store, generate & autofill strong passwords
- Keepass (offline, open-source)
- Bitwarden (free, secure, sync across devices)

Demo - Bitwarden

Multifactor Authentication

2FA

- SMS OTP (least secure)
- Authenticator apps (Google Auth, Aegis, Authy)
- Push notifications (Okta, Duo)

Hardware Keys

- Uses FIDO2 standard
- Examples: **YubiKey, SoloKey**
- Strong phishing-resistant authentication
- Works with Bitwarden, Google, Microsoft, GitHub, etc.

Demo - 2FA Hardware Keys

- Recommended TOTP App: Ente Auth - FOSS, Sync across devices, No lockin
- Recommended MFA App: Duo
- Checkout 2fa.directory website for the services that support various MFA methods

Backup Codes

> **Caution**
> Losing access to your two-factor authentication (2FA) method can lock you out of your accounts

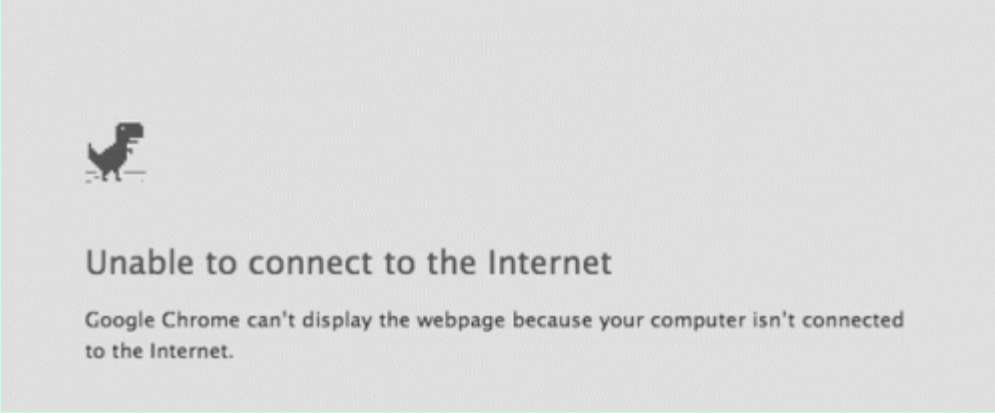
- Always save backup codes when enabling 2FA
- Store in a safe place (paper/secure vault)
- Bitwarden security readiness kit

Passkeys

Passkeys offer a way of confirming you are who you say you are without remembering a long, complicated password, and in a manner that's resistant to common attacks on passwords like phishing and dictionary attacks.

- Next-gen passwordless authentication
- Uses device biometrics (fingerprint, FaceID)
- Backed by Google, Apple, Microsoft
- You an save your generated passkeys in password managers
- passkeys.directory

DNS - Domain Name System

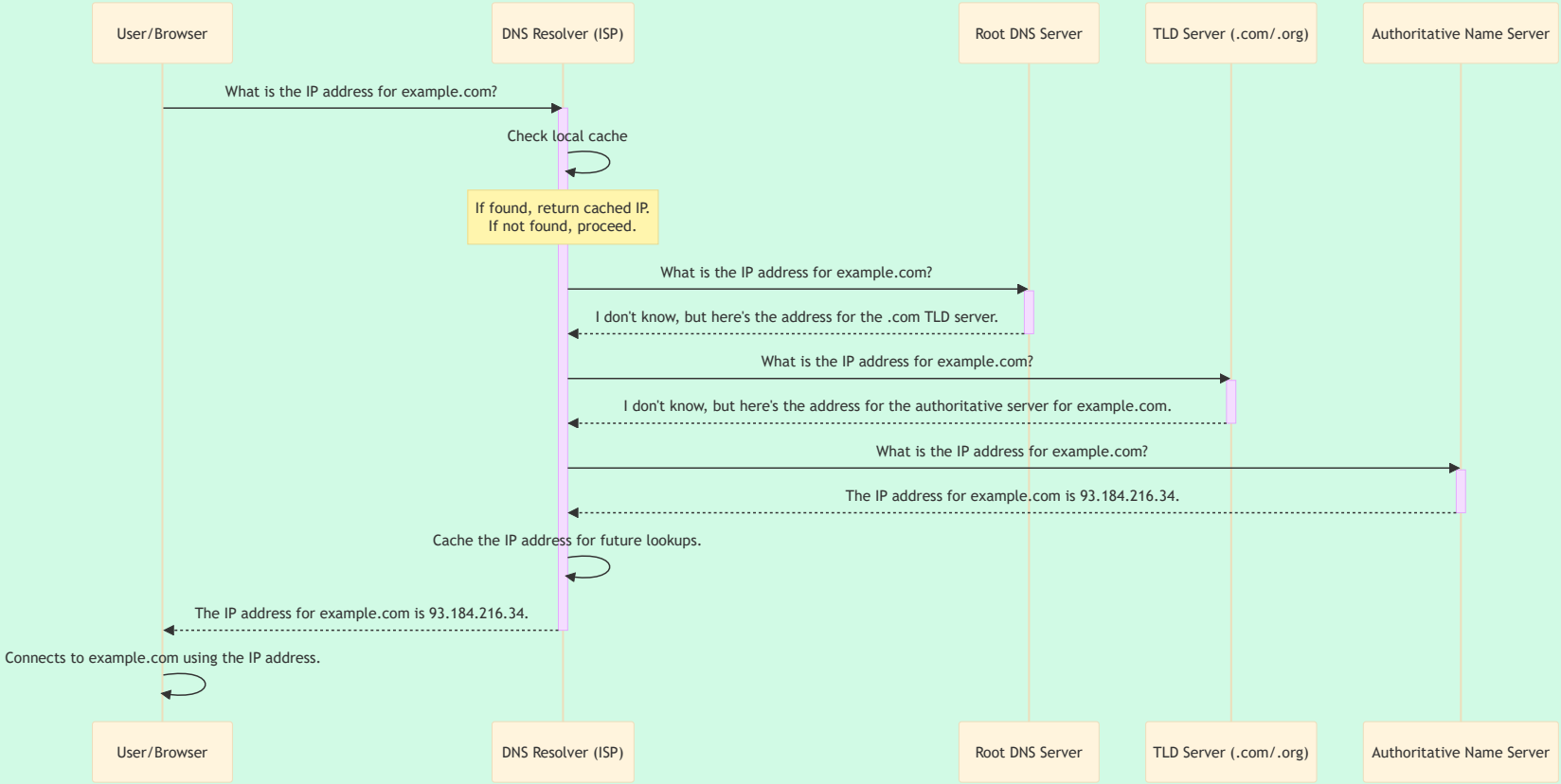


What is DNS

- Domain Name System = Internet’s Phonebook
- Converts names (google.com) → IP addresses

How DNS Works

1. User enters website URL
2. Request sent to DNS resolver
3. Resolver queries authoritative servers
4. IP address returned → browser connects


User/Browser
DNS Resolver (ISP)
Root DNS Server
TLD Server (.com/.org)
Authoritative Name Server
What is the IP address for example.com?
Check local cache
If found, return cached IP.
If not found, proceed.
What is the IP address for example.com?
I don't know, but here's the address for the .com TLD server.
What is the IP address for example.com?
I don't know, but here's the address for the authoritative server for example.com.
What is the IP address for example.com?
The IP address for example.com is 93.184.216.34.
Cache the IP address for future lookups.
The IP address for example.com is 93.184.216.34.
Connects to example.com using the IP address.
User/Browser
DNS Resolver (ISP)
Root DNS Server
TLD Server (.com/.org)
Authoritative Name Server

DNS -> Cybersecurity

DNS Filtering

How DNS filtering works

- A user requests a domain (e.g., badsite.com).
- The DNS filtering service checks that domain against threat categories or allow/block lists.
- If the domain is flagged (malware, phishing, etc.), the request is blocked.
- If it’s clean, the DNS query proceeds normally.

Using Free DNS filtering service

- controld.com
- recommended DNS providers
- **Paid:** NextDNS, ControlD

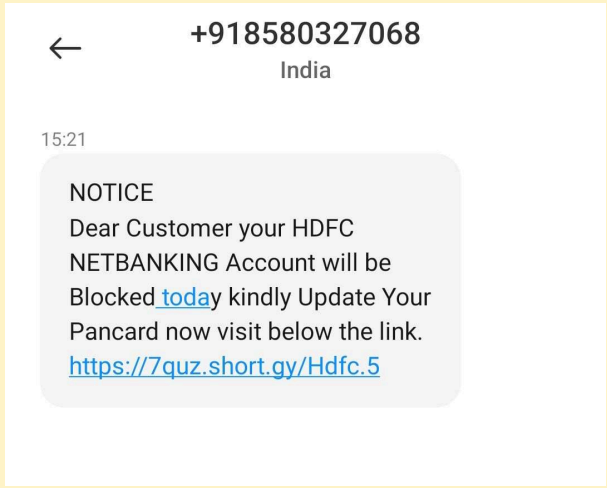
NextDNS Features

- Blocks ads & trackers
- Parental controls (safe search, category filters)
- Privacy

DNS

Demo - NextDNS

Spams & Scams


+918580327068
India
15:21
NOTICE
Dear Customer your HDFC NETBANKING Account will be Blocked today kindly Update Your Pancard now visit below the link.
https://7quz.short.gy/Hdfc.5

Fighting Spams and Scams

Spam

Spam refers to unwanted messages sent in large numbers through email, texts, or social media

- Marketing spam
- Social media spam
- SMS spam
- Robocall spam

Scam

A scam is a scheme meant to cheat people or businesses out of money or personal information

- Phishing scams
- Identity theft scams
- Investment scams
- Fake lottery scams
- Tech support scams
- AI impersonation scams

Identify Scam / Spam / Phishing

- Check sender email / phone number
- Hover over URLs → look for mismatches
- Spelling errors, urgent tone
- Unrealistic promises
- Unsolicited offers
- Threats and pressure
- Suspicious attachment

Congratulations, ! You've won a grand prize of $250,000 in our International Lottery Draw. To claim your prize, reply with "CLAIM" and your full name and address

Hi, this is Chris from Microsoft Support. We've detected a critical virus on your computer. To prevent permanent data loss, we need to connect to your computer remotely to fix it. You'll need to provide your account information first

How to protect yourself - Identity Theft

Identity theft is the act of wrongfully obtaining someone's personal information (that defines one's identity) without their permission. The personal information may include their name, phone number, address, bank account number, Aadhaar number or credit/debit card number etc.

- Do not close the browser window without logging out of the account.
- Do not save your username and password in the web browser
- Permanently delete all documents downloaded on computers in cybercafé.
- Never provide details or copy of identity proofs (e.g. PAN Card, Aadhaar Card, Voter Card, Driving License, Address Proof) to unknown person/organization.
- Do not share sensitive personal information (like Date of Birth, Birth Place, Family Details, Address, Phone Number) on public platforms.

How to protect yourself - Social Engineering

Attackers play with the minds of the user to trap them with lucrative offers. Once trapped, the attackers can exploit the victim by either stealing money or stealing sensitive personal information (name, Aadhaar details, bank account details etc.) or harm the victim in any other way. The entire basis of this kind of attack is to make the victim fall into their trap by sending fake e-mails, calls or SMSs

- Always verify the correctness of the domain of the e-mail ID, for example, all government websites have “.gov.in” or “.nic.in” as part of their web address.
- Do not respond to messages from unknown source requesting personal or financial details even if it assures credit of money into your bank account.
- Do not get petrified if you receive a call stating that your card is blocked. Bank will never convey such information on call.
- Do not share your PIN, password, card number, CVV number, OTP etc. with any stranger, even if he/she claims to be bank employee. Bank will never ask for any vital information.

How to protect yourself - Social Media Frauds

Social Media has become an integral part of our lives. One can understand the entire history of an individual through their social media profile and can even predict future events based on patterns in the past. This poses a threat to an individual as unwanted access to social media profile can cause loss of information, defamation or even worse consequences such as physical/sexual assault, robbery etc. Hence, protection and appropriate use of social media profile is very important.

- Do not accept friend requests from strangers on social networking sites
- Restrict access to your profile. Social media sites offer privacy settings for you to manage who can view your posts, photos, send you friend request etc.
- Ensure your personal information, photos and videos are accessible only to your trusted ones.
- Discuss safe internet practices with your friends and family regularly.
- Monitor your kid’s activity on internet/social media. Enable parental controls on computer/mobile devices.

How to protect yourself - Mobile App Frauds

Mobile applications are widely used not only for entertainment but also for ease and convenience to perform day-to-day tasks such as bill payments, bank accounts management, service delivery etc. As a result, these applications are more prone to cyber-attacks

- Always install mobile applications from official application stores or trusted sources.
- Scrutinize all permission requests thoroughly, especially those involving privileged access, when installing/using mobile applications. For example, a photo application may not need microphone access.
- Regularly update software and mobile applications to ensure there are no security gaps.

How to protect yourself - Online Banking Frauds

As all the banking services are shifting towards online platforms, cyber frauds related to banking are also increasing.

- Register your personal phone number and e-mail with your bank and subscribe to notifications. These notifications will quickly alert you on any transaction and the unsuccessful login attempts to your net-banking account
- Always review transaction alert received on your registered mobile number and reconcile with the amount of your purchase.
- Do not save your usernames and passwords in the web browser. Use Password Managers!
- Always be sure about the correct address of the bank website and look for the ‘‘lock’’ icon on the browser’s status bar while visiting your bank’s website or conducting an online transaction. Always be sure ‘‘https’’ appears in the website’s address bar before making an online transaction. The ‘‘s’’ stands for ‘‘secure’’ and indicates that the communication with the webpage is encrypted.

How to protect yourself - General

- Always download software or applications from known trusted sources only. Never use pirated software on your systems/devices.
- Always change the default admin password on your Wi-Fi router to a strong password known only to you. In addition, always configure your wireless network to use the latest encryption.
- Be cautions while browsing through a public Wi-Fi and avoid logging in to personal & professional accounts such as e-mail or banking on these networks.
- Always use virtual keyboard to access net-banking facility from public computers; and logout from banking portal/website after completion of online transaction.
- Note the IMEI code of your cell phone and keep it in a safe place. The operator can blacklist/block/trace a phone using the IMEI code, in case the cell phone is stolen.
- Discuss safe internet practices with your friends and family regularly! Motivate them to learn more about cybercrimes and safe cyber practices.
- Do not store unencrypted data on cloud services

Cybercrime Reporting

- ☎️ Dial **1930** for fraud & cybercrime help
- 🌐 National Cyber Crime Reporting Portal - cybercrime.gov.in
- To report lost or stolen mobile phones, file a First Information Report (FIR) with the police. Post filing the FIR, inform Department of Telecommunications (DoT) through the helpline number 14422 or file an online compliant on Central Equipment Identity Register (CEIR) portal by visiting https://ceir.gov.in. After verification, DoT will blacklist the phone, blocking it from further use. In addition to this, if anyone tries to use the device using a different SIM card, the service provider will identify the new user and inform the police.

Government Apps

- **Sancharsathi** (report spam SMS/calls, check registered mobile nos. on your name)

Privacy & Digital Wellbeing

> Arguing that you don’t care about privacy because you have nothing to hide is like saying you don’t care about free speech because you have nothing to say
>
> - Edward Snowden

Data - The New Oil

How Big Tech Collects Your Data

- Web Browsing & Search History
- Social Media Activity
- Smartphone Apps & Permissions
- Voice Assistants & Smart Devices
- Purchases & Online Shopping
- Location Tracking
- Emails & Cloud Storage

How Big Tech Uses Data

- Targeted Advertising
- Product & Service Improvement
- Profiling & prediction
- Selling to data brokers

⚠
Android Manifest example

ⓘ
Watch the documentry 'The Social Dilemma'

How to Protect Your Privacy Online

- Block ad and trackers using DNS filtering
- Use VPN
- Prefer Web Apps
- Disable Location Services When Not Needed
- Limit App Permissions
- Use Encrypted Messaging & Email Services
- Read TOS

Social Media Alternatives

- **Fediverse** (Mastodon, Lemmy, Pixelfed)

Chat Alternatives

- Signal, Matrix, Element

Privacy Guides

🌐 privacyguides.org

Digital Wellbeing →

It’s OK to be Bored

- Constant stimulation = digital fatigue
- Allow downtime for mental health

Some Tips

- Turn Off Notifications
- Keep Mobile Phone Out of Reach
- Limit Screen Time

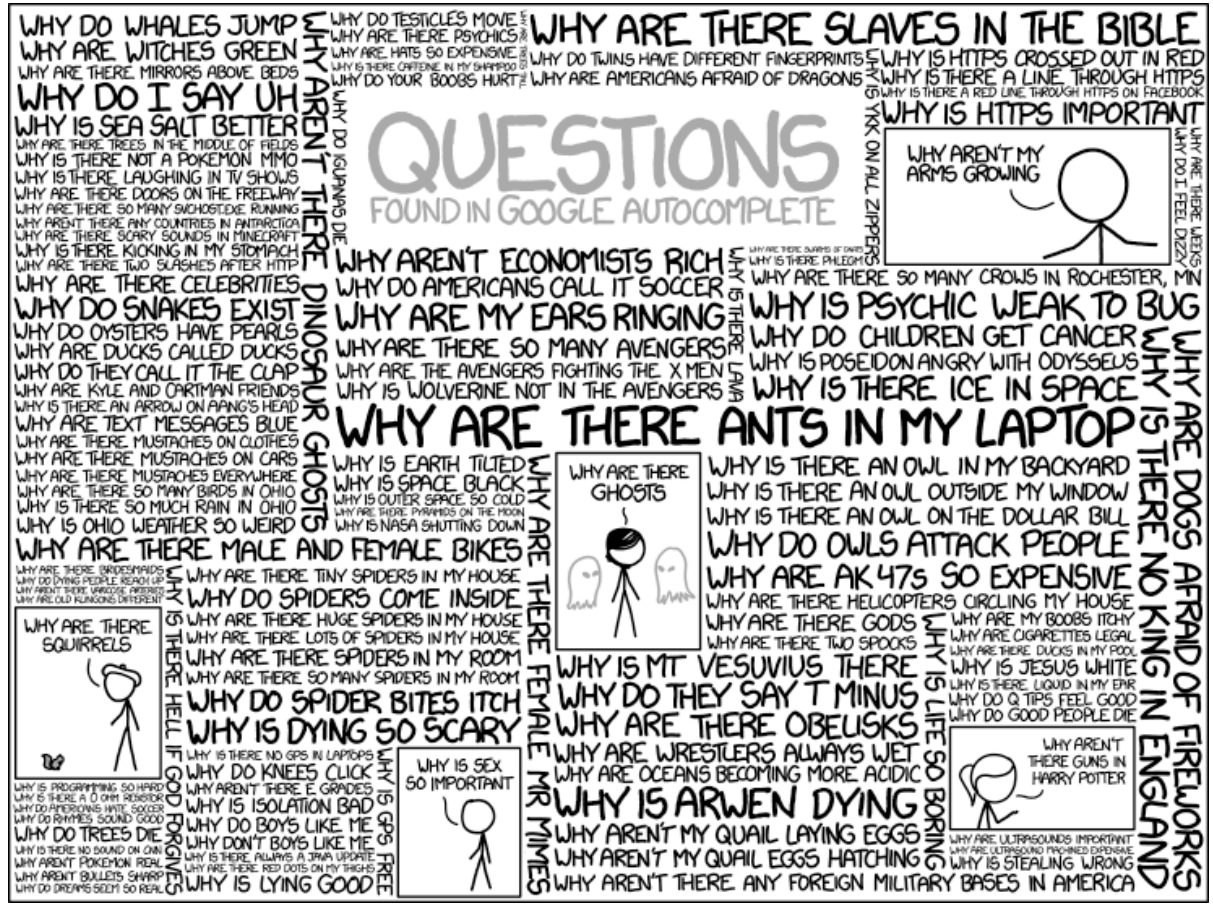
Key Takeaways

- Use Password manager
- Compulsarily use one form of 2FA - TOTP << Duo << Hardware Keys
- Keep MFA recovery codes safe
- Use DNS filtering service
- Mind your privacy
- Turn off Notifications
- Stay Updated

Interesting Links

- 🎧 Darknet Diaries podcast
- 🌐 Privacyguides.org
- IntelTechniques
- 💌 Proton.me (Mail, Drive, VPN)
- Reddit: r/privacy, r/selfhosted, r/degoogle
- Cyberawareness
- 🔎 VirusTotal

Any Questions ?



Thank You!

Stay Vigilant, Stay Secure 🔒