PESU ISFCR

ZERO DAY CYBERSEC

Introduction to cybersecurity and best practices

Cybersecurity

“Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation”

Source: NIST CSRC Glossary https://csrc.nist.gov/glossary/term/cybersecurity

Security mindset

- Trust, but verify.
- Stop. Think. Proceed.
- If you see something, say something.

CIA Triad

- Confidentiality: limiting who can see or read sensitive information.
- Integrity: maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle.
- Availability: information or device should be consistently and readily accessible

Vulnerability lists & databases

- MITRE Common Vulnerabilities and Exposures (CVE) list - https://cve.mitre.org
- NIST National Vulnerability Database (NVD) - https://nvd.nist.gov/

Social Engineering

- An attempt to trick someone into revealing information that can be used to attack systems or networks.
- Can be achieved through multiple ways:
  - Phishing: A technique for attempting to acquire sensitive data, through a fraudulent solicitation in email or on a web site, in which the perpetrator pretends to be a legitimate business or reputable person.

Types of phishing

- Spear phishing: Attack against a specific individual.
- Whaling: Going after executives in a company.
- Smishing(SMS-ishing): Phishing using SMS.
- Vishing(Voice Mail): Phishing using voice mail.

MFA

For stronger security and to ensure it’s really you, we use something known as Multi-Factor Authentication (MFA). This is something you

- Know
- Are
- Have

Something that you know

- Usually passwords
- Most popular means of authentication as of today
- Strongest and the weakest form of authentication
- Use passphrases instead of passwords
- Use unique and random ones everytime

Password Managers

- Generate long, random and unique passwords
- Single master password
- Passwords are usually stored in encrypted files

Examples: KeePassXC, Bitwarden etc.

Bitwarden

- Open source
- Third party security audits
- Multiplatform and cloud based so can be accessed from anywhere (can be self hosted)
- Free plan has the basic features that a password manager should have.
- https://bitwarden.com/

KeePassXC

- FOSS
- Local – Database stored on device
- Highly customisable and has tons of features – Encryption type, Key derivation function etc.
- Cross platform softwares
- Android – KeePassDX, Keepass2Android
- You are responsible to backup and store the database
- https://keepassxc.org/

Disadvantages

- Cannot access passwords if you forget the master password
- Single point of failure
- Weak master password defeats the purpose

Someone who you are

- Physical characteristic of a person
- Fingerprint
- Face
- Iris

Something that you have

- Device that you own

  Examples FIDO 2FA keys, smartphone etc

SMS 2FA

- User gets an OTP (One Time Password) via a sms.
- Not very secure these days
- Declining method of 2FA
- Still better than no 2FA

TOTP

- Time based One Time Passwords
- Use standardized algorithms that take current time as input
- Adoption rate growing
- Considerably secure
- App based – Aegis, andOTP (FOSS), Google, MS Authenticator (proprietary) etc.

FIDO 2FA keys

- Fast Identity Online
- Hardware USB keys
- Work across devices
- Latest standard - FIDO2
- Nitrokey, Yubikey etc.
- Disadvantages
  - Costly

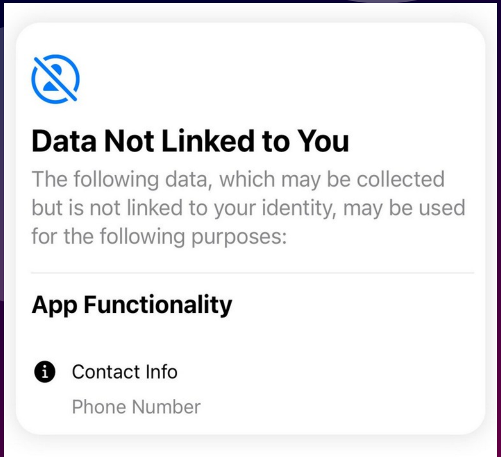
E2EE

- End to End Encryption – Only sender and receiver can view the message
- Uses public key cryptography
- PGP (Pretty Good Privacy) used for encrypting emails

Useful services and tools

- Signal – Best instant messaging app – uses open source Signal Protocol – considerd gold standard of privacy)
- Email – Protonmail, Tutanota
- Matrix – Decentralized platform
- Veracrypt – Create an encrypted vault
- Cryptomator – Encrypt files before uploading to cloud

App Labels



Data Not Linked to You

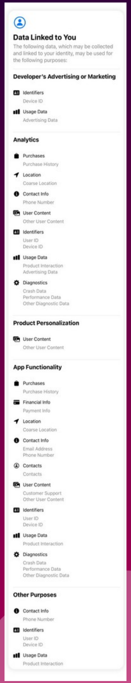
The following data, which may be collected but is not linked to your identity, may be used for the following purposes:

App Functionality

Contact Info

Phone Number

Signal App label



Data Linked to You

The following data, which may be collected and linked to your identity, may be used for the following purposes:

Developer's Advertising or Marketing

Identifiers
Device ID

Usage Data
Advertising Data

Analytics

Purchases
Purchase History

Location
Coarse Location

Contact Info
Phone Number

User Content
Other User Content

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Product Personalization

User Content
Other User Content

App Functionality

Purchases
Purchase History

Financial Info
Payment Info

Location
Coarse Location

Contact Info
Email Address
Phone Number

Contacts
Contacts

User Content
Customer Support
Other User Content

Identifiers
User ID
Device ID

Usage Data
Product Interaction

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Other Purposes

Contact Info
Phone Number

Identifiers
User ID
Device ID

Usage Data
Product Interaction

Whatsapp App Label

Source – Apple App Store

QnA

Thank You!