Gov-X Innovation Challenge 2021

Privacy 101

Christo Esterhuizen

Cybersecurity Engineer

Christo Esterhuizen

Cybersecuirty Engineer

Background:

I have been technically involved in the Cybersecurity industry since 2013. Focussing on engineering, architecting, maintaining, and administrating Cybersecurity systems throughout my career.

Today’s talking points

- Privacy 101 Introduction
- Data Privacy and why it matters
- Security: How do we protect all this information?
- Final thoughts

1.

Privacy 101

Introduction

Privacy 101 Intro

CONFIDENTIAL

What does data privacy mean?

- Right to have control over how your personal information is collected and used

Most conversations revolves around…

- Massive data breaches
- Social Networking
- Targeted advertising

Facebook data breach of 50million users in 2018

Privacy 101 Intro continued

Privacy and Security go hand in hand

- Data privacy focuses on the use and governance of personal data
- Security focuses on protecting data from melicious actors and exploits for profit

Data privacy uses polcies and is enforced by regulations (GDPR and POPI).

Security is the technology that is implemented for protecting private data.

2.
Data privacy

Why does it matter?

Personal Information

What does it include?

- Name, Date of birth, Email, Telephone Number, Marital Status, ID number
- Family Members
- Medical Status
- Employment
- Education

Risk?

- Identity theft
- Take out loans against your name
- Compromise accounts
- Potential financial loss

Gathered by attackers using Phishing Email campaigns or data breaches.
Typically sold and used for the above mentioned including SPAM calls and advertising.

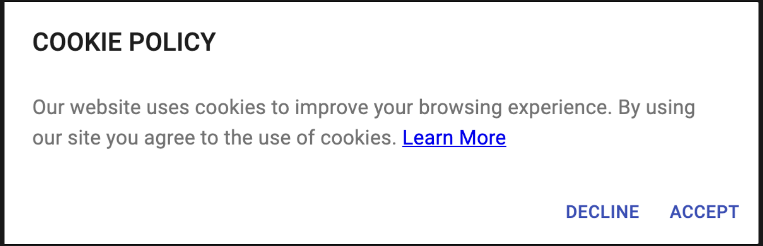
Browsing Pattern and Website visits

What does it include?

- Internet activity monitored by
    - ISP (Internet Service Provider)
    - Cookies (bits of text that are downloaded and stored by your browser)
    - Browser add-ons (used to enhance user experience, example ad-block)

Risk?

- Tailored advertising
- Tracking
- Recording activities



COOKIE POLICY

Our website uses cookies to improve your browsing experience. By using our site you agree to the use of cookies. Learn More

Gathered to be used acros varions platforms for marketing.
These actions are considered as interference and intrusive.

Message and Email content

What does it include?

- Instant Messaging service (WhatsApp, Telegram, WeChat)
- Email

Risk?

- Hijacking of accounts
- Can be used to SCAM friends and family
- Potential financial loss

Gathered by attackers using Phishing Scams, Socail Engineering or Data breaches.
Messanger services has the potential to record our communication with other people.

Online Purches and Financial Information

What does it include?

- Online transactions with Credit Card
- Online transactions via financial services like
    - PayPal
    - Google Pay
    - WePay

Risk?

- Unauthorised transactions
- Clone Cards can be made
- Potential financial loss

Gathered by attackers using Man in the middle attacks, Compromised payment portals, Card Skimming or Data breaches.
Typically sold and used for the above mentioned.

Medical Records

What does it include?

- Name, Date of birth, Email, Telephone Number, Marital Status, ID number
- Family Members
- Employment
- Very sensitive personal medical information

Risk?

- Identity theft
- Take out loans against your name
- Compromise accounts
- Potential financial loss
- Exposure of sensitive information

Gathered by attackers using Phishing Email campaigns or data breaches.
Typically sold and used for the above mentioned including SPAM calls and advertising.

3.
Security

How do we protect all this information?

Regulations

Governments are enforcing the protection of personal data.

This is being done by regulations like GDPR (General Data Protection Regulation) and POPI (Protection of Personal Information Act).

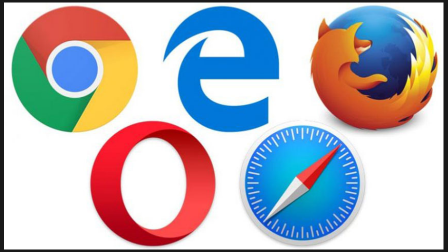
- GDPR technical requirements for businesses
  - Protect personal data
  - Resistance to malicious code & hacks
  - Evaluate personal data risk
  - Build data protection by design

In short, it sets some conditions for responsible parties to lawfully process the personal information of users.

Secure your browsers

Get in the habit to do and check the following:

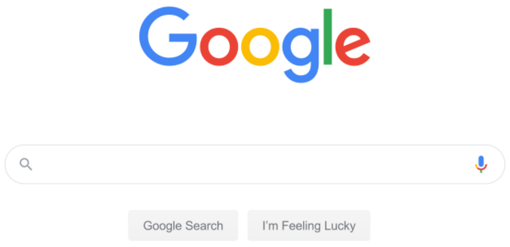
- Clear out Cookie caches
- Clear out History
- Prevent browsers from storing Cookies at all
- Use HTTPS over HTTP when browsing



This will improve your Security when using browsers like Google Chrome, Safari, Firefox, Microsoft Edge.

These changes should be fairly quick to implement without making major changes to your surfing habits.

Search Engines



Google is the best search engine to use! Right?

- Make use of algorithms based on your data to provide "personalized" experiences
- Browsing histories and search queries can be used to create crossover user profiles
- Detailing our histories, clicks, interests, and more, and may become invasive over time

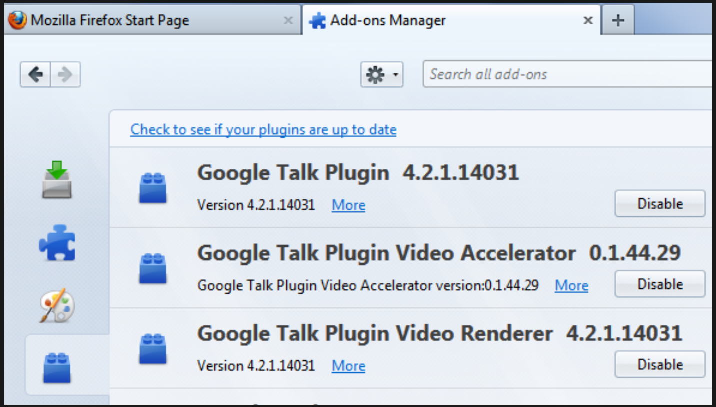
Ever purchased a tablet and then see adverts for tablets frequently?
There's a reason for that!

To prevent such data from being logged, consider using an alternative that does not record your search history and blocks advertising trackers. These options include DuckDuckGo, Qwant, Startpage, and the open source Searx engine.

Browser Plugins

Consider using the following!

- HTTPS Everywhere
- Disconnect
- Blur



Check to see if your plugins are up to date

Google Talk Plugin 4.2.1.14031
Version 4.2.1.14031 More

Google Talk Plugin Video Accelerator 0.1.44.29
Google Talk Plugin Video Accelerator version:0.1.44.29 More

Google Talk Plugin Video Renderer 4.2.1.14031
Version 4.2.1.14031 More

How does this help?

These browser plugins helps improve encryption, awareness and protection of your data.

Public Wi-Fi

Should you use public Wi-Fi?

- Typically no authentication needed
- Public Wi-Fi's are most often not secured
- Man-in-The-Middle attacks in order to eavesdrop and steal your information
- Hackers may be able to access your information (email, financial and account details)

How do I get around this?

- Use your mobile device as a Wi-Fi hotspot
- Ensure to set a password on your mobile device Wi-Fi hotspot
- If you have to use a Public Wi-Fi, do not access anything valuable like online banking

VPNs

What is a VPN?

- Virtual Private Network
- Used to create a secure tunnel between browsers and web servers
- Data is encrypted
- Results in your IP and location becoming hidden

VPN’s help mask your presence online.

VPN’s typically comes in a Free and Paid version. Paid version will always be more trustworthy, free version and often slow and will limit certain functionality.

Password and Vaults

This is a must!

- Always use complex passwords
- Password vaults stores all your complext passwords
- Password vaults will also assist in generating these passwords for you

What is the most popular password vault?

By now you may have seen or heard of LastPass. This is the most well known password manager.

Two factor Authentication

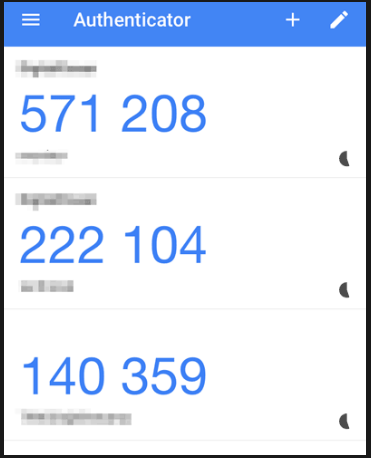
What is it?

Two-factor authentication (2FA), also known as two-step verification, is a widely-implemented method of adding an extra layer of security to your accounts and services after you have submitted a password.

Used by most social media platform already like Facebook, Twitter, Instagram, Snapchat etc.

Common methods

- SMS message
- Fingerprint
- Iris scan
- PIN number
- Pattern
- Authenticator App



571 208

222 104

140 359

Protect Mobile devices

By now we all spend most of our day on our mobile devices and we store more and more information on them (photos, videos, accounts, emails etc.)

This means that mobile devices are a rich source of information for attackers.

Consider adding an extra layer of protection

- Anti-virus security software
- Update software and application regularly
- Lock your device!
- Use remote wipe features if your mobile devices is stolen

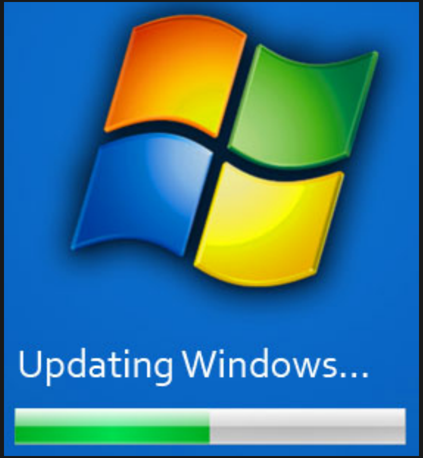
Software update

Update package downloaded
uccessfully. During installation
annot use your device a
ergency calls. A
data wi

Patch!

Patches are important

- Fixes flaws and vulnerabilities
- Improves performance
- Adds functionality (extra protection in some cases)
- Prevents attackers from using it as a point of entry



Install your Windows and Mobile device patches as soon as they become available.

They are crucial in preventing attackers from exploiting flaws and vulnerabilities in software that we use daily.

Encryption

What is it?

- Encryption is a way to encode information to make it unreadable by unauthorized parties.

How is it done?

- Encryption uses algorithms to scramble your information. It is then transmitted to the receiving party, who can decode the message with a key. There are many types of algorithms, which all involve different ways of scrambling and then decrypting information.

Why is encryption important?

- It helps protect private information, sensitive data, and can enhance the security of communication between applications and servers.

Social Networks

Social networks can be major sources of data leaks. It is not just friends and family that might be stalking you across social media bur prospective employers or shady characters may be doing so as well. So, it is important for you to lock down your accounts to make sure only the information you want to be public, is public.

View and change your security settings

Facebook, Twitter, Instagram etc. has security features to further lock down your accounts. To name a few -

- Login verification (Enable!)
- Location settings (Disable!)
- Privacy and Safety settings (Enable!)
- Advert preferences (Disable!)

4.
Final thoughts

> “You have to fight for your privacy or you lose it.”
>
> \- Eric Schmidt
>
> (Google CEO 2001 – 2011)

THANK YOU!

Any questions?

You can find me at

christo_esterhuizen@trendmicro.com

Source: https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/