

u3a Computing Group

Alan Hopwood, 2 March 2023

Agenda



Next Month



Welcome

Current News, Issues and Questions

Topic List

Password Managers

AOB and Follow up

Future Topics

Topic	Votes
Password Managers & Access security	7
Use of USB Sticks	4
Acceptance of Cookies	3
Using the PDF format (editing, programming)	3
What are VPNs	3
Android - laptop integration	2
Alternatives to MS Office on Windows	2
Exploring Microsoft Account	2
Laptop vs Tablet	1
Printing from an Android Tablet	0

Presentation

Password Managers

*PASSWORD MANAGERS ARE the vegetables of the internet. We know they're good for us, but most of us are happier snacking on the password equivalent of junk food. For nearly a decade, that's been "123456" and "password"—two of the most commonly used passwords on the web.
(Wired)*

Presentation Agenda

Password Managers

- Password related Security Risks
- Defenses
 - Internet basic security - SSL
 - VPNs (do they help?)
 - Multi-factor authentication
 - Passkeys (the future?)
- Password Managers
 - Functionality
 - Available systems & selection

Password Risks

Password Managers

1. **Phishing**: Sending a fraudulent email, posing as a trustworthy party to get you to reveal your personal information
 - **Regular Phishing**: email from "goodwebsite.com" asking you to "reset your password".
 - **Spear phishing**: A hacker targets you specifically with an email that appears to be from a friend, colleague, or associate. It has a brief, generic blurb ("Check out the invoice I attached and let me know if it makes sense.") and hopes you click on the malicious attachment.
 - **Smishing and vishing**: You receive a text message (SMS phishing, or smishing) or phone call (voice phishing, or vishing) from a hacker who informs you that your account has been frozen or that fraud has been detected. You enter your account information and the hacker steals it.
 - **Whaling**: You or your organisation receive an email purportedly from a senior figure in your company. You don't check the email's veracity and send sensitive information.

Password Risks

Password Managers

- **Brute Force Cracking**
 - Use automated tools to generate billions of passwords; trying each one of them to access the user's account and data until the right password is discovered.
 - Will try all combinations of letters, numbers, and symbols according to the password rules, until they find the one that works.
 - Brute force attacks aren't usually successful when conducted "online" due to password lockout rules that are usually in place.
- **Dictionary Attack**
 - A type of brute force attack, dictionary attacks rely on our habit of picking "basic" words as our password, the most common of which hackers have collated into "cracking dictionaries." More sophisticated dictionary attacks incorporate words that are personally important to you, like a birthplace, child's name, or pet's name.

Password Risks

Password Managers

- Reuse of Passwords and Use of Compromised Passwords
 - if one website or system's data is compromised, it's likely that attackers will obtain users' credentials. If a user uses similar passwords across different platforms, the attacker can access their data on other sites and networks as well.
 - Digital Shadows researchers have found 6.7 billion unique logins—combinations of usernames and passwords—on the dark web.
- Keyloggers
 - Keyloggers are a type of malicious software designed to track every keystroke and report it back to a hacker. Typically, a user will download the software believing it to be legitimate, only for it to install a keylogger without notice.

Password Risks

Password Managers

- Password Recovery/Reset Systems
 - Systems that allow users to recover or reset their password if they have forgotten it can also let malicious actors do the same. Remember, a forgotten password mechanism is just another way to authenticate a user and it must be strong!
 - Online systems that rely on “security questions” such as “birthday” or “pet’s name” are often too trivial for authentication as attackers can easily gain basic personal details of users from social networking accounts.

Password Risks

Password Managers

Stupidity:

- From public data breaches, collected and analysed 15,212,645,925 passwords
 - 12,995,630,435 were not unique
 - And the top 10 passwords were:
- 
- 123456
 - 123456789
 - qwerty
 - password
 - 12345
 - qwerty123
 - 1q2w3e
 - 12345678
 - 111111
 - 1234567890


Defenses

Password Managers

- SSL
- VPNs
- Good password management
- multi factor authentication
- Biometrics
- passkeys (future)

SSL - Secure Sockets Layer

Password Managers

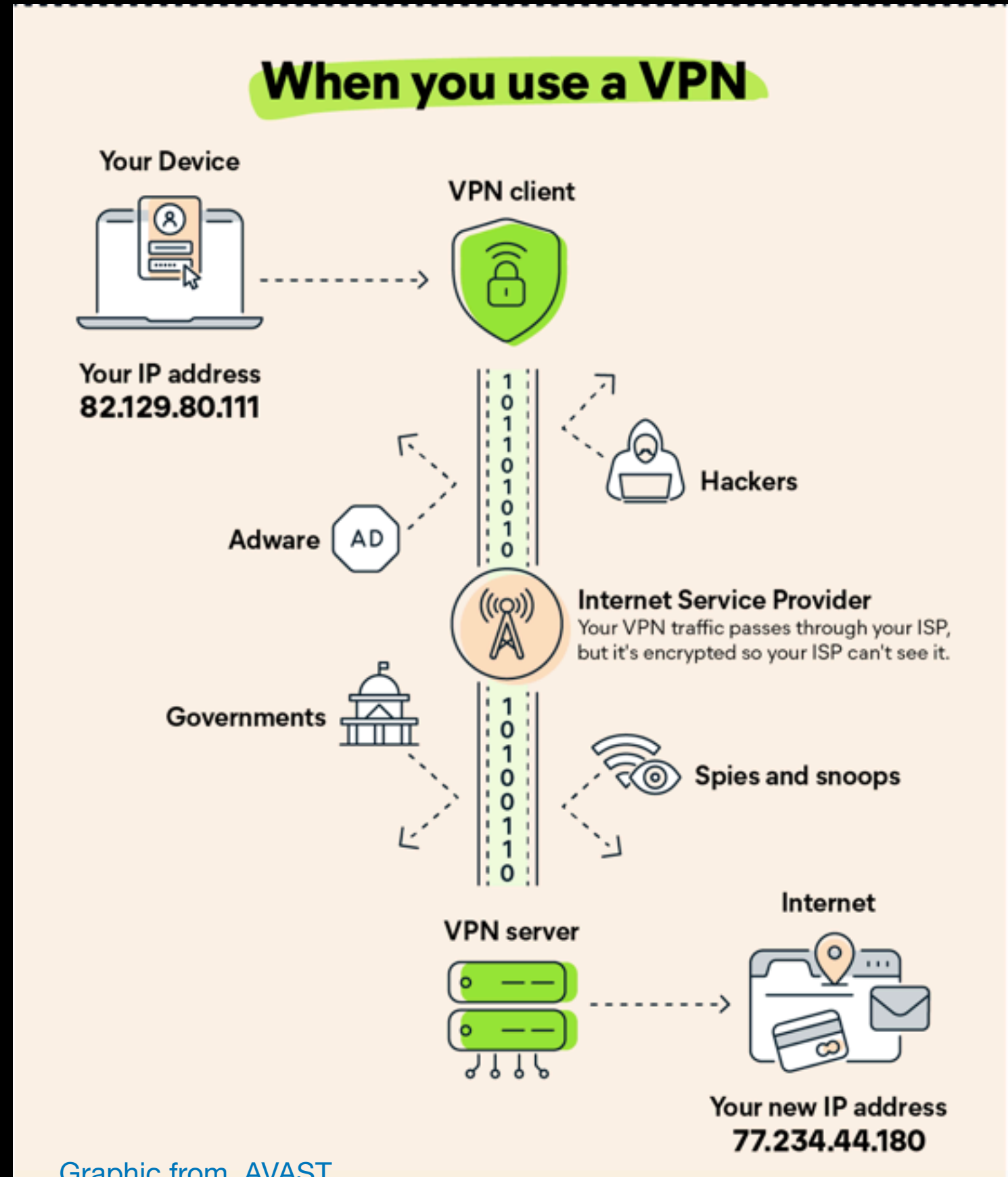
- SSL is the standard technology for keeping an internet connection secure.
- Works between your web browser and the website you are connecting to.
- For a website to use SSL, it must have an SSL certificate.
- Websites address (URL) show as https:// rather than http//. Also show a lock icon and/or green URL. 
- Your connection to an SSL certified website is secure / encrypted.
- But this does not validate the website itself - a Website scammer can buy an SSL certificate.
- There are different levels of SSL certificate. Click on the lock to see the certificate!



VPN - Virtual Private Network

Password Managers

- A VPN establishes an encrypted connection between your computer and a server on the internet, providing a private tunnel for your data and communications.
- A VPN service allows you to connect to the internet from their server using their IP address.
- Your onward connection does not identify where or who you are.



Multi-factor identification

- A method by which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence:
- Most common 2FA types - password plus...
 - Text / voice based to confirm you have your mobile phone
 - Bank card reader to confirm you have your bank card
 - Biometrics - fingerprint or face recognition on phone

Types of Factors for 2FA



Knowledge
tokens include
PINs and security
questions.



Hardware
tokens are physical
objects, like bank
cards or USB drives.



Biometrics use
fingerprints
and **voices** for
identification.



Passkeys (the future?)

Password Managers

- Standard promoted by the FIDO (Fast Identity Online) alliance (members include Apple, Google, Microsoft)
- An alternative to passwords
- An authenticator app on phone or pc
 - Validates the user
 - Face recognition or fingerprint to validate user (Your biometric data does not leave your device)
 - USB FIDO key
 - Password or pin on phone but....
 - The app uses public-key cryptography to authenticate your access to websites and apps
 - More secure than 2FA.
- Some Banks and Paypal already allow use of passkeys.

Status Check

Password Managers

- We have established
 - SSL protects the connection
 - 2FA doubles your security
 - FIDO should remove the problem some day
 - Passwords are as strong or weak as we make them
- Need to:
 - Have long unique unguessable passwords
 - Each password only used for one website/app
 - Stored where no one can access it.
 - Make sure you are connecting to the genuine website.

Password Manager Functionality

Password Managers

A password manager is essentially an encrypted digital vault that stores secure password login information you use to access apps and accounts on your mobile device, websites and other services.

Common PM functionality

- ***Secure Vault****
- Biometric access to vault
- ***Password creation****
- Changing the recipe
- ***Synchronisation across devices****
- ***Quick access to login info****
- ***Auto form filling (Web Browser extension)****
- ***Weak password warnings****
- Duplicate password warnings
- ***Warn of compromised passwords****
(found in data leaks or Dark Web)
- Storage of other sensitive information such as for bank cards.

*all PMs discussed have these

Available

Password Managers

There are a lot of password managers!
This selection is taken from articles in CNET & Wired.
All of these are good!

- Google Password Manager
- Apple Keychain
- ~~Other Browser PMs~~
- Bitwarden
- 1Password
- Dashlane
- KeyPassXC
- Nordpass
- Keeper

Google Password Manager

Password Managers

- Safe, completely free and easy to use, especially if you don't require extensive functionality...
- Browser tool rather than a full password manager
- Browser specific - available if you are using Chrome and have a Google account
- Generates strong passwords, but does not allow recipe changes.
- On the Google passwords page, users can:
 - View all active saved passwords,
 - View and edit details and delete stored information.
 - Use the password checkup option to make sure passwords are as secure as possible
 - See potential security problems from passwords that have been involved in known breaches.
- Not useful outside of the World of Google

Apple Keychain

Password Managers

- Safe, completely free and easy to use, if you mainly use Apple devices.
- Built into every Mac, iPhone and iPad
- Available on iCloud for Windows - Chrome and Edge Browsers, but more limited and not as easy to use.
- Generates strong passwords, but does not allow recipe changes.
- Automatic synchronisation between devices
- Automatic login to websites
- Similar functionality to Google - e.g. identify passwords involved in known breaches.
- Designed work automatically - user interface on mac is poor - iPad is better.

Other Browser PMs

Password Managers

- Most Browsers have a rudimentary password manager
- Risk is that the company does not invest enough to keep ahead of the threats.

Bitwarden

Password Managers

The open-source Bitwarden's free tier handles all expected password manager tasks with surprisingly few limitations. Its paid tier adds security and storage tools at an extremely low price for the category (PCMag)

- Devices: Mac, Windows, Linux, Android, IOS
- Browsers: Google Chrome, Mozilla Firefox, Opera, Microsoft Edge, and Safari.
- Supports all the functionality mentioned
- A little less user friendly than 1Password

1Password

Password Managers

- One of the top password managers - no free version, \$36 pa
- Apps for Mac, Windows, Linux, Android and Web
- Supports Chrome, Edge, Firefox, Brave.
- Unlimited devices, unlimited passwords
- Alerts for compromised websites and vulnerable passwords
- Store credit & debit cards, online banking info, Paypal logins
- Travel mode - removes sensitive data while crossing borders & restores with a click after arrival.

Bitwarden vs 1Password

Password Managers

- Bitwarden and 1Password are two of the best password managers in the market
- They offer a variety of features common to top password management tools. But, where Bitwarden's open-source nature allows it to keep up with current password security trends more easily, 1Password offers greater usability and password sharing and recovery features.
- 1Password has a wider variety of features compared to Bitwarden, it's easy to use and get started

Feature	Bitwarden	1Password
Security and encryption	Yes	Yes
Usability	Not as easy	Easy to use
Password sharing	Yes	Yes
Master password recovery	No	Yes
Password Generator	Yes	Yes
Cost	Free	\$36 pa

Available

Password Managers

Depending on your needs, take your pick!

- Google Password Manager
 - Apple Keychain
 - ~~Other Browser PMs~~
 - Bitwarden
 - 1Password
 - Dashlane
 - KeyPassXC
 - Nordpass
 - Keeper
- for the Google world
for an Apple environment
check before using
more functionality & free
functionality, ease of use
alternative to 1Password
DIY option - self hosted & free
alternative to 1Password
alternative to 1Password

Thank You