Personal Security and Digital Safety

BY BRIAN OBILO

whoami

- Certified Security Analyst.
- Cybersecurity Engineer/ Researcher/Trainer
- NCSTP Graduate - Cohort 1.
- Mozilla Open Leaders 6 and X Alumnus.
- Gamer.
- Avid reader.

Follow me on Twitter: @brian_obilo

Scope

What we'll cover today

01

Personal Security

02

Password security and good password practices.

03

Multi-Factor Authentication

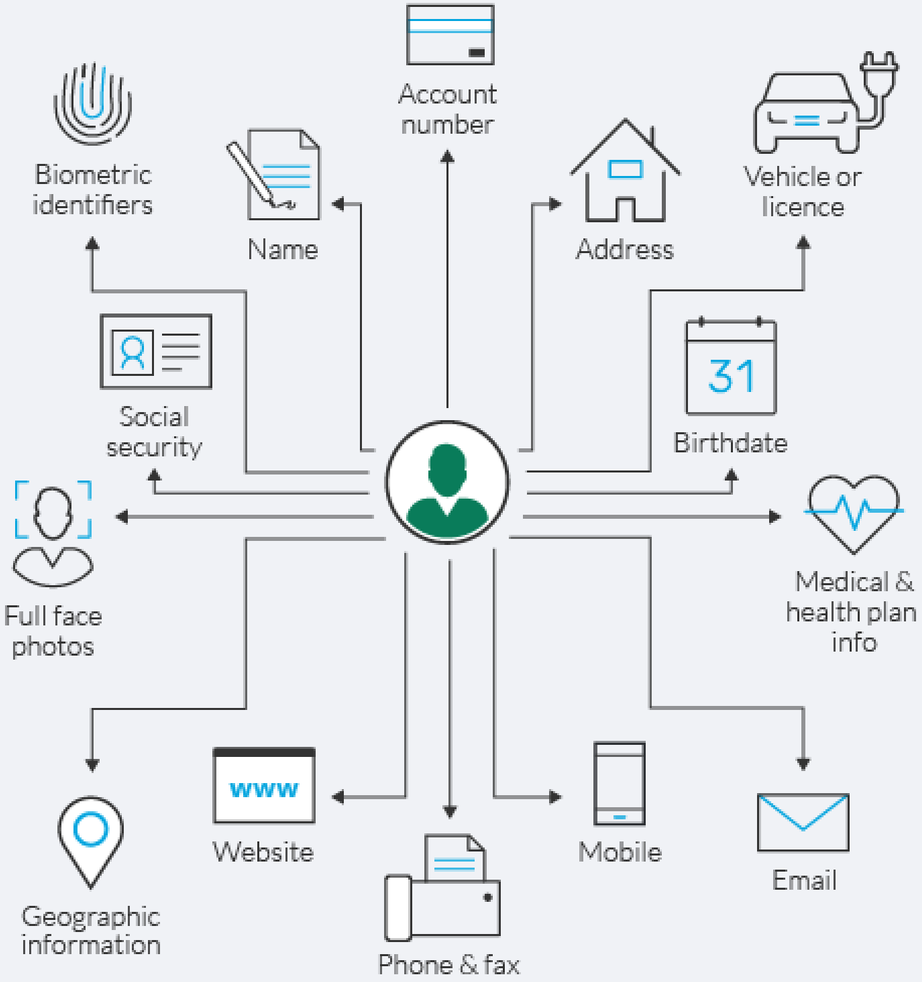
Personal Security

What is PII?

This refers to any information that can lead to locating and contacting an individual and identifying that individual uniquely.

These include:

- Full Name and Parents' names
- National ID & Passport Number
- Bank account numbers
- Phone number
- Home address
- Driving License/Vehicle registration number
- Biometrics



What you can do

- Don’t respond to unsolicited requests for personal information by phone, mail or online.
- Adopt a clean desk policy.
- Not leaving computers on and not password protected.
- Install firewalls and virus-detection software on your home computer.
- Store personal or sensitive information in a safe place at home and at work.
- Always review your receipts. Promptly compare receipts with account statements and look for any unauthorized transactions

What you can do (cont.)

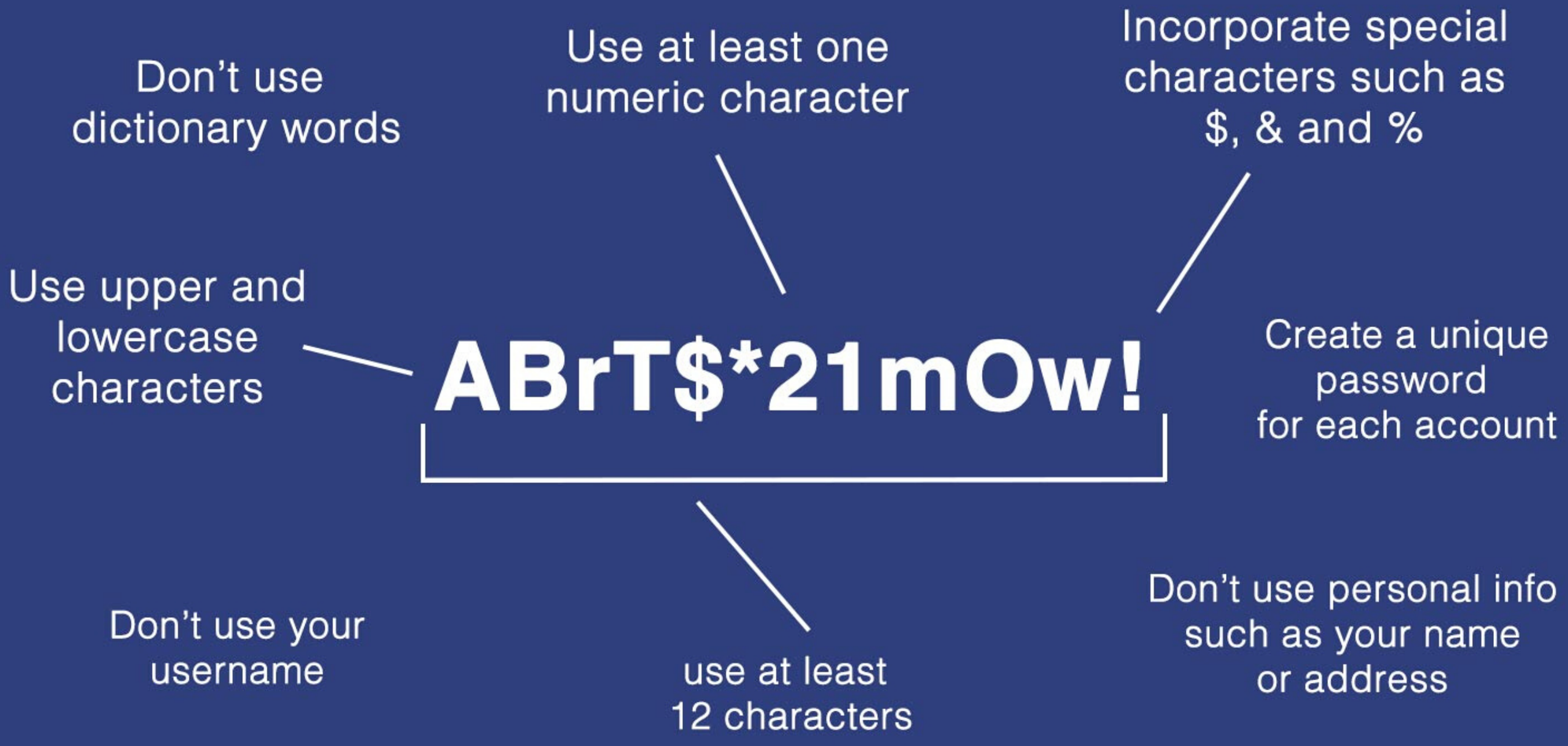
- Watch out for shoulder surfers specifically when entering sensitive information such as when entering passwords at your computer or pins at ATMs.
- Shred receipts, credit offers, account statements, and expired cards, to prevent "dumpster drivers" from getting your personal information.
- Adopt good password security practices to protect all of your accounts and devices.

Password Security

How are passwords dicovered ?

- Interception.
- Brute force attacks.
- Dictionary attacks.
- Keylogging.
- Shoulder surfing.
- Manual guessing.
- Cracking Security Questions.
- Phishing and coercion.
- Data breaches.
- Stealing passwords .
- Password spraying.

Creating a Complex Password



How to not secure your password

How to secure your password

- Make sure you use different passwords for each of your accounts.
- Be sure no one watches when you enter your password.
- Always log off if you leave your device and anyone is around.
- Check your password strength. If the site you are signing up for offers a password strength analyzer, pay attention to it and heed its advice.
- Avoid entering passwords on computers you don’t control (like computers at an Internet café or library).
- Avoid entering passwords when using open/unsecured Wi-Fi connections (like at the airport or coffee shop).
- Separate personal from work. Use separate passwords for personal and work accounts.

How to secure your password (cont.)

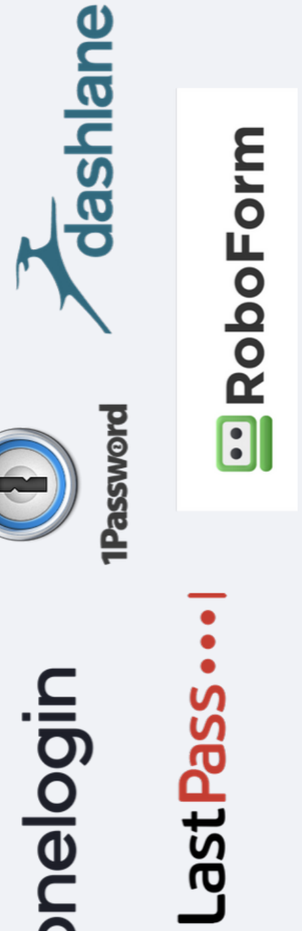
- Don’t tell anyone your password. Your trusted friend now might not be your friend in the future. Keep your passwords safe by keeping them to yourself.
- Do use at least twelve characters of lowercase and uppercase letters, numbers, and symbols in your password.
- Don’t bunch up your special characters. Put your digits, symbols, and capital letters spread throughout the middle of your password, not just at the beginning or end.
- It’s important to always use **Multi Factor Authentication(MFA)** on all of your accounts. MFA is a method to double check whether it is you trying to access the account.

Password Managers

You can use a password manager to store your passwords for you. It has both pros and cons.

Password manager pros:

- Using the same credentials for each account is dangerous as it creates one point of failure. Password managers help avoid this.
- Good password managers encrypt all your personal data in case someone hacks the PM software directly; the hacker might get your passwords but they won't know who the passwords belong to.
- Password Managers can keep you up to date with the latest breaches and advise you if any accounts may have been affected/hacked.
- Can use offline password manager (not stored on the web/not a web browser plugin like KeePass
- Humans can be unreliable as they can come up with bad/weak passwords, forget their password, or are genuinely disinterested in their own security.



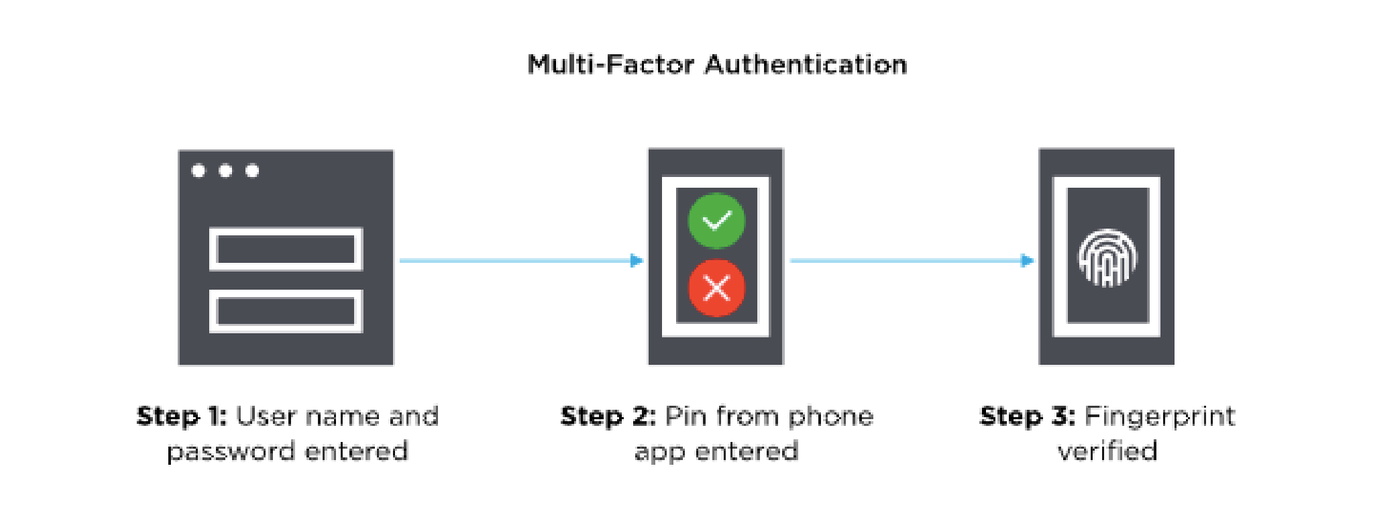
Password Managers

Password manager cons:

- Single point of failure - if someone gets hold of your master password, they have all your passwords.
- Password manager programs are a target for hackers.
- It’s not easy to login using multiple devices.
- If the main password is used/typed/saved on a computer with malware, your main password can compromise all your other passwords controlled by the Password Manager - all your passwords are only as secure as your master password.
- Not all PM’s are adequately encrypted which can render the whole process of setting one up useless.

Multi-Factor Authentication

- Multi-Factor Authentication (MFA) is a security system that verifies a user's identity by requiring multiple credentials.
- Rather than just asking for a username and password, MFA requires other—additional—credentials, such as a code from the user's smartphone, the answer to a security question, a fingerprint, or facial recognition.
- An example of Multi-factor Authentication:



Types of Authentication Factors

There are three types of authentication factors:

01

Things you know (knowledge), such as a password or PIN

02

Things you have (possession), such as a badge or smartphone

03

Things you are (inheritance), indicated through biometrics, like fingerprints or voice recognition

2FA Products to use

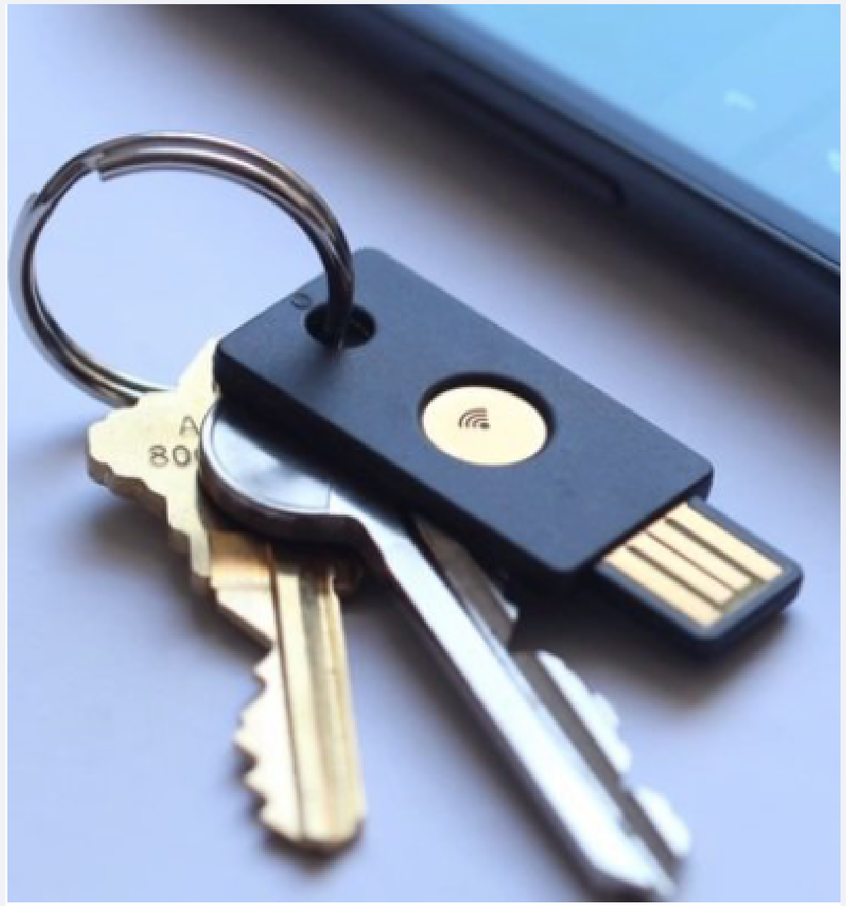
Apps to consider:

1. Google Authenticator (highly recommend).
2. Lastpass Authenticator
3. Microsoft Authenticator
4. Authy: Best for multiple devices.

Hardware to consider:

1. Yubico Authenticator
2. Titan Security

Bonus: Google and Apple's on device prompts.



Q&A