Scam

Subject: Stop struggling with passwords and make them stronger.

If you feel like you spend half your life clicking "Forgotten Password," you are not alone.

For years, we were told to create complicated passwords like P@55w0rD!, change them every 90 days, and never write them down. The problem? That advice made things difficult for humans, but easy for computers to crack.

The guidance has changed. Here is how to make your passwords stronger *and* easier to remember.

1. Length beats complexity: Use "Three Random Words".

Computers are very good at guessing standard substitutions (like swapping an 'a' for an '@' or an ‘I’ for a ‘1’). They are much worse at guessing length.

Instead of a short, complex jumble of characters, combine three random words together. Remember with passwords LONGER is STRONGER.

- **Bad:** Tr0ubl3! (Hard to type, difficult to remember, easy for hackers to crack)
- **Good:** RedHouseMonkeys (Easier to type, easy to remember, very hard to crack)

This method creates a password that is long enough to keep criminals out, but simple enough for you to remember. You can add numbers or symbols if the website requires it (e.g., 1RedHouseMonkeys!), but the length is the most important part.

2. The Golden Rule: Don't reuse your passwords

This is the most common mistake we all make. If you use the same password for your Facebook, your email, and your online shopping, a hacker only needs to crack one to access them all.

Think of it like a master key: if you lose it, you lose access to your house, your car, and your office all at once.

If you can’t remember different passwords for everything, prioritize your Email and your financial accounts.

Your email account is the gateway to your digital life. If a criminal gets into your email, they can reset the passwords for all your other accounts. Give your email a unique, strong, **"Three Random Words"** password that you use nowhere else.

3. Let your browser take the strain

You don't actually need to remember every single password for your many online accounts.

Most modern web browsers (like Google Chrome, Safari, or Edge) and many mobile phones will offer to **save your password** when you log in.

- **Say "Yes" to this for all accounts other than your email and financial accounts. To be ultra safe you should still memorise those.**
- It is much safer to have unique, complex passwords saved in your browser than to use "Password123" everywhere because you're afraid of forgetting it.
- You can also use dedicated "Password Manager" apps, which work across all your different devices.

A CAUTIONARY NOTE – Don’t save passwords on shared devices. Only save them on a device that only you use and ensure that the device itself is secured, often by way of a PIN, fingerprint or facial recognition. This means that if anyone picks up your device, they cannot easily gain access to its contents.

Summary: Your 3-Step Action Plan

- **Update your Email Password:** Change it to **Three Random Words** combined together. LONGER IS STRONGER.
- **Stop Reusing Passwords:** Ensure your banking and email passwords are unique (not used anywhere else).

- **Save Them:** Let your browser / password manager or phone remember the rest of your passwords for you.

More information on improving you password security can be found here - Improve your password security - Stop! Think Fraud

Reporting

If you think you have been a victim of cybercrime, please report the incident to Action Fraud via phone (0300 123 2040) or via their website at https://www.actionfraud.police.uk

If you think you have lost money or given out sensitive financial information to scammers, immediately alert your bank / financial institution. Call them right away to inform them of the suspicious incident. You can quickly reach many UK banks' fraud departments by calling **159**.

If you've received a suspicious email, please forward it to the NCSC's suspicious email reporting service (SERS) at report@phishing.gov.uk . Forward suspicious text messages onto 7726.

Reply | Share | Rate

Message Sent By
Mick Harrison
(Devon & Cornwall Police, Cyber Protect Officer, Devon & Cornwall)

Your Devon and Cornwall Community Messaging account...

Area Insights | Update Preferences | System Support | Unsubscribe

Powered by neighbourhood ALERT

You are receiving this message because you are registered on Devon and Cornwall Community Messaging. Various organisations are licensed to send messages via this system, we call these organisations "Information Providers". Please note that this message was sent by The Police and that The Police does not necessarily represent the views of Devon and Cornwall Community Messaging or other Information Providers who may send you messages via this system.

You can instantly review the messages you receive and configure which Information Providers can see your information by clicking here, or you can unsubscribe completely, (you can also review our terms and conditions and