Charities Unlocked:
How To Make Your Passwords Stronger

24%

Almost a quarter of charities said they experienced a cyber breach in the last 12 months

Source: Cyber Breaches Survey 2023, DSIT

Passwords are an important part of cyber security but they can be easy for cyber criminals to crack

- The most common base term found in compromised passwords was 'password'
- The second most common base term was 'admin'

(Source: Specops Weak Password report, 2023)

How to create strong passwords

Tips from the Global Cyber Alliance Toolkit for Mission-based Orgs

1. Make it memorable but hard to crack

The longer and more unexpected your passwords are, the better: **DON'T USE 'PASSWORD'.**

Think of at least two random objects and insert a verb to make it funny (e.g. dinosaur riding a time machine.) The funnier you make the phrase, the more memorable your password will be.

Add some combination of special characters (e.g. £, #, &, etc.) and you've got an unlikely, yet memorable password.

2. Mix it up, securely (with Password Managers)

65% **of people re-use their passwords across multiple sites**
(Source: Google Security Survey, 2019)

If you've used the same password across different accounts, cyber criminals only need one password to access all your accounts that use that same password.

To help you store and manage unique login credentials for each website or app that you use, make use of Password Managers, which store your passwords safely and securely in one location.

3. Audit your passwords

Online tools such as Specops Password Auditor and Have I Been Pwned? can identify password-related vulnerabilities and tell you if your password has been compromised.

Storing your passwords in a spreadsheet on your computer or a note on your phone causes a different security problem!

- LEARN MORE

4. Employ Multi-factor Authentication (MFA or 2FA)

MFA via an app (like Google Authenticator or Microsoft Authenticator) is **significantly more secure** than using SMS due to the risk of SIM-swapping attacks, so if you have a choice, **use an app!**

Multi-factor or Two-Factor Authentication adds an extra level of security to passwords.

It requires users to authenticate their login details via a code that is sent to them on another account.

If an attacker discovers a password, they won't be able to access the associated account without also compromising the other factor.

5. Create a clear password policy

Create a list of password dos and don'ts, explaining the risks.

Share tips to create better, stronger passwords (and provide password managers to help them remember them)

Create a uniform policy for sharing passwords internally – add extra checks (such as a video call) to ensure that a password request is legitimate.

For more resources to keep your charity cyber secure, check out the .ORG Learning Center from PIR and the Global Cyber Alliance toolkit

CHARITY DIGITAL

.org