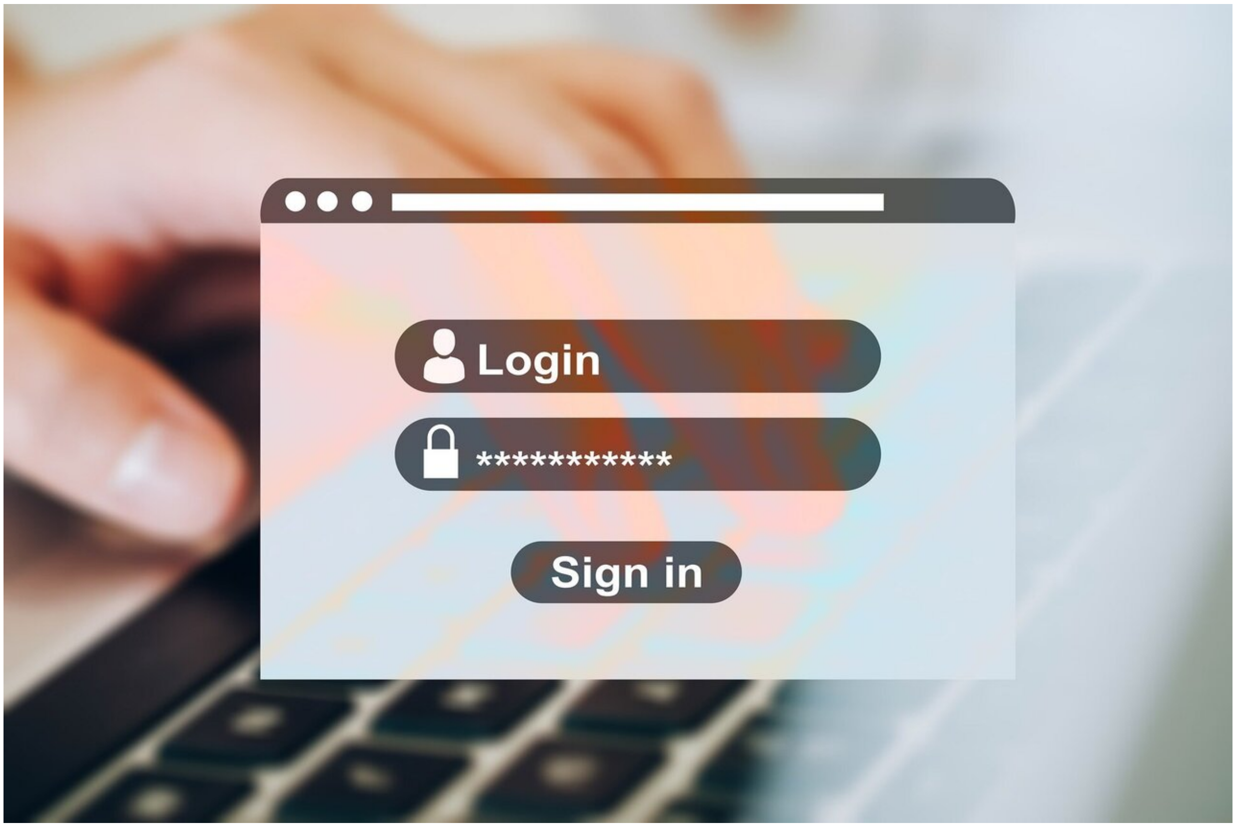
TechXplore

How to avoid being hacked: Start by upping your password game—'12345' doesn't cut it

June 17 2024, by Thembekile Olivia Mayayise



Credit: Pixabay/CC0 Public Domain

If you type the term "password cyberattack" into Google News, the results will show just how often cyber criminals are getting hold of important data belonging to companies and individuals. Weak passwords are a big part of the problem. For instance, in 2023 technology security firm Nordpass reported that "123456" was the most common password in Nigeria, and the second most common password in the whole world.

Thembekile Mayayise is a cybersecurity professional and researcher. The Conversation Africa asked her to outline how employers and employees can improve their password safety.

Why is password security so important?

The spike in cyberattacks leading to system breaches and data leaks has compelled a review of access control strategies. The question has shifted from whether cyberattacks will occur to when and how they will happen.

Passwords and usernames remain a key point of vulnerability as they are still used for access and authentication. Too many people use weak and recycled passwords.

A report by cybersecurity firm Sophos found that the "number of cyber attacks on businesses in South Africa, Kenya and Zambia increased by 76% in 2023." This comes at a huge cost.

Each year various sources publish lists of the most used passwords. Research by NordPass often highlights predictable choices like "123456," "admin," "12345678" and "password."

These passwords can be cracked in less than a minute by highly skilled hackers and those with basic hacking skills. Confidential information is then exposed to theft, deletion or tampering. AI tools are making hacking easier.

In some organizations, passwords never expire, creating opportunities for unauthorized access. In many instances, compromised passwords result in online identity theft. Nor are password-saving features, such as websites offering to auto-save when you create a new account, a flawless solution. Despite the convenience, these platforms pose a risk of credential exposure.

What can companies do differently?

A password policy and corresponding standards should be developed and implemented to meet the company's cybersecurity objectives. How this is done depends on the organization and the type of business. For example, financial institutions and credit card companies may find the Payment Card Industry Data Security Standard to be most appropriate.

Others might find the guidelines provided by the US National Institute of Standards and Technology or ISO/IEC 27001 security standards useful. These standards are used globally.

Companies must ensure that employees are fully informed about the policies and procedures related to password use and that they understand their responsibilities. They should therefore:

- conduct regular awareness campaigns to promote safe password practices and address potential password threats
- follow best practice security standards for user accounts management and password control
- incorporate password-strength meters to assist users in generating more secure passwords
- consider adopting multi-factor authentication, which requires two or more pieces of evidence to authenticate a user—for example a password and facial or retina recognition
- ensure that the password files are encrypted
- conduct regular audits to monitor and ensure compliance with password policies and standards.

What about individuals?

Individuals can enhance their online safety—both at work and in their private life—by remaining vigilant and informed about the latest threats that could compromise password security. In organizational settings you should:

- know and follow organizational policies and standards for safe password use
- participate in awareness and training sessions
- report any suspicious security incident to the ICT help desk or follow your organization's incident management process
- keep your login credentials safe and secure
- log out after every session, especially when you're using a shared computer
- use passwords which are strong and unlikely to be guessed by attackers
- avoid using sequential characters or repetitive phrases for passwords, recycled or easily guessable passwords such as dictionary words
- check if the chosen password is not already on the list of breached or common passwords
- change your password whenever a compromise is suspected
- use encrypted password manager tools to store passwords safely.

What are the biggest password no-nos?

Don't use basic or easily guessable passwords, such as common dictionary words. Users should aim for a password not shorter than 12 characters long, a combination of alpha numeric (letters and numbers) and special characters, and lower and upper cases (small and capital letters) and keep it confidential.

It's also important not to reuse passwords across different accounts.

Don't use auto-fill or save your passwords on websites especially on shared computers.

Avoid sharing passwords or revealing them to others, particularly with colleagues in the workplace. If you have to share a password, ensure that it is authorized by the manager and that the details are documented for auditing purposes.

Never give password details over the phone to individuals claiming to be IT technicians without proper verification.

Some of the ways to verify the authenticity of the call are as follows:

- confirm the ticket number the caller is referencing
- ask the caller to send an official email to your account, especially if you don't have issues accessing a computer
- if an internal telephone number is being used, check the authenticity of the call
- request identification details from the caller such as their name, office location, department and reporting lines.

Provided by The Conversation

Citation: How to avoid being hacked: Start by upping your password game—'12345' doesn't cut it

(2024, June 17) retrieved 26 June 2024 from https://techxplore.com/news/2024-06-hacked-upping-password-game-doesnt.html