Read or listen to this article online

Scan the QR code to open this article on XO.PL

Article source:

https://xo.pl/it-made-fun-sec-passwords

IT SECURITY

Passwords and MFA: a lock, a key and a second security guard

The Golden Password Hotel had just opened a new wing. Three hundred rooms, three lifts and one Manager who had decided that keys were unnecessarily complicated. He ordered a universal key, engraved “SECRET” on its keyring, then attached it to the pen on the reception desk so nobody would lose it. 🔑🏨🤣

— Why does that key open the safe as well? — asked Agnes from Accounting.

— BECAUSE IT'S UNIVERSAL! THAT'S OPTIMISATION!

— Why is it next to the guest book?

— SO IT'S EASY TO FIND!

Gregory examined the key.

— Congratulations. You've invented the password “123456” in metal.

One key for every door

A notebook lay on reception. The booking system, email, security cameras and accounting software all shared the same password: `Hotel2026!`.

— IT HAS AN EXCLAMATION MARK! — the Manager protested.

— So does the burglar's keyboard — Agnes replied.

— If a password leaks from one service, criminals can try it elsewhere — Gregory explained. — That's **credential stuffing**: using stolen login details across other websites. That's why **every account should have a unique password**.

— AND HOW AM I SUPPOSED TO REMEMBER THEM ALL?!

— You can't even remember your room number.

— BECAUSE YOU KEEP CHANGING IT!

— You've occupied the same room for three years — Agnes replied.

Long and unpredictable, not three exclamation marks

Room 404 had a sign: “Every password must contain a capital letter, a digit, a special character and a small amount of personal suffering.”

— I WROTE IT MYSELF! — the Manager boasted.

— We've already met the last requirement — Agnes sighed.

Gregory pointed at `P@ssw0rd!`.

— Replacing “a” with “@” or “o” with zero doesn't rescue a common password. What matters is **length, unpredictability and uniqueness**. Password managers can generate long random passwords. If you need to type one manually, a suitably long passphrase of randomly selected words can work well if the service supports it.

— I'VE GOT ONE! “THE MANAGER IS ALWAYS BRILLIANT”!

— The most predictable sentence in the building — Agnes said.

— BUT IT'S LONG!

— Length alone isn't enough when everybody knows your favourite sentence. And don't use educational examples as real passwords.

A receptionist with a thousand keys

In the next room, a receptionist guarded an enormous cabinet. Every compartment had a different key, and the catalogue was locked inside a vault.

— Meet our **password manager** — Gregory said. — It keeps logins in a protected vault, can generate unique passwords and helps fill them in. People don't need to memorise hundreds of strings.

— So I only remember one master password? — Agnes asked.

— Usually, plus extra protection for the manager where available. The master password must be strong. And check the recovery options in advance.

— I'LL PUT A SPARE KEY UNDER THE DOORMAT! — the Manager announced.

— No. Not in a shared spreadsheet or on a note beside the monitor, either. Store recovery codes separately and securely.

— WHERE EXACTLY?

— I'm certainly not explaining that in front of every guest.

The second security guard at the lift

A guard stood beside the lift. The Manager showed his key but wasn't allowed through.

— WHAT?! I HAVE THE KEY!

— Somebody might have stolen it — the guard replied. — I need another proof.

— I'M THE MANAGER!

— That's what every second visitor tells him — Gregory said.

— This is **MFA — Multi-Factor Authentication**. We can combine something you know, like a password; something you have, such as a device or security key; and something you are, such as a biometric characteristic.

— Are two passwords two factors? — Agnes asked.

— No. They're both from the knowledge category. **Two login steps aren't necessarily two-factor authentication.**

— I HAVE TWO THUMBS! — announced the Manager.

The guard opened his notebook and began drafting a transfer request.

Text messages, app clocks and annoying prompts

Three stations were arranged upstairs: “SMS”, “Authenticator Code” and “Approve on Phone”.

— Which is best? — Agnes asked.

— It depends on the threat and what's available. **SMS codes** are usually better than a password alone, but numbers can be hijacked and codes can be stolen. **TOTP** codes come from an app using a shared secret and the current time. They don't need incoming texts, but you can still be fooled into typing them on a fake website.

— And the “Approve” notification?

— Convenient, but only approve sign-ins you initiated. Criminals sometimes flood users with requests, hoping they'll click one out of frustration. That's **MFA fatigue**, also called push bombing.

The Manager's phone buzzed.

— IT WANTS APPROVAL!

— Are you signing in?

— NO!

— Then deny it and report the unexpected request.

It buzzed again.

— BUT IT'S ASKING VERY NICELY!

— Persistence isn't proof of identity — Agnes said.

A key that recognises the real hotel

Gregory placed a model hotel next to the real one. The sign said “G0lden Password Hotel”, with a zero.

— Almost identical — the Manager observed.

— Exactly. **FIDO2 security keys and properly implemented passkeys** use cryptography linked to the genuine website. A lookalike domain shouldn't receive a signature intended for the real one.

— So I don't need to type a password?

— With a passkey, often not. Your device signs a challenge with a private key, and the service checks it using a public key. The private key shouldn't be transmitted to the website. A PIN or biometric check can unlock it locally.

— DOES MY FINGERPRINT GET SENT TO THE HOTEL?! — the Manager asked.

— Not in this model. Biometrics usually stay on the device for local verification.

— SO NO CROOK CAN EVER FOOL US NOW!

— Not quite. Somebody can still trick staff into transferring money, exploit weak account recovery or compromise a device. Resistance to **login phishing** isn't immunity to every scam.

The hotel shouldn't keep the password written inside the safe door

— How does the server know my password is correct? — Agnes asked.

— A well-built server shouldn't keep plaintext passwords. It stores **properly calculated password hashes with unique salts** and verifies the supplied value. Purpose-built password hashing algorithms include Argon2id, properly configured scrypt and bcrypt.

— What about plain SHA-256?

— A fast hash alone isn't suitable password storage. Attackers can try huge numbers of guesses if they steal the database.

— I'LL HASH IT THREE TIMES! — suggested the Manager.

— Please don't invent your own cryptography — Gregory replied.

— YOU NEVER LET ME HELP!

— That's why the server room has its own lock.

A new password every month, another number every month

The Manager proudly presented his policy: “Mandatory password changes every thirty days.”

— So staff create `Hotel2026!01`, then `Hotel2026!02` — Agnes observed.

— **Forcing routine changes without a specific reason isn't a universal best practice** — Gregory explained. — Change passwords when they're compromised, suspected to have leaked or there's another justified reason. Unique passwords, checks against known compromised choices, login rate limits and MFA are more useful.

— What if I forget my password?

— Then use secure account recovery. Questions like “What's your dog's name?” can be easy to guess.

— MY DOG'S NAME IS SECRET!

— Not anymore — Agnes said.

An emergency exit the burglar uses first

Before closing, Gregory asked to see backup authentication methods.

— If we lose a phone or security key, we need an account recovery plan that doesn't give access to strangers. That might mean **recovery codes stored safely, a backup hardware key or another officially supported method**.

— THEN WHY HAVE A SECOND GUARD?! — protested the Manager.

— Because a crook who can't enter through the front door may tell reception he's lost his key. If we issue replacements to anyone who cries loudly enough, security is just decoration.

— So we verify people during account recovery too? — Agnes asked.

— Exactly. Companies should decide who may approve resets and how to verify and record them.

— I KEEP MY SPARE KEY UNDER A FLOWERPOT! — the Manager announced.

— Again?!

— BUT IT'S A DIFFERENT FLOWERPOT!

Checking out

By the following morning, the hotel had unique room keys, a password manager, extra authentication and an emergency plan. The Manager called a press conference.

— FROM NOW ON, NOTHING CAN EVER BE STOLEN!

— We never promised that — Gregory replied. — Strong, unique passwords, a password manager and MFA make accounts harder to take over. Passkeys and FIDO2 keys can make login phishing much harder. But we still need updates, reasonable permissions and incident response.

— I've enabled a second factor! — Agnes said.

— Excellent.

— And a password manager!

— Even better.

— AND I HAVE A SPARE KEY! — cried the Manager.

— Where?

He leaned forward conspiratorially.

— I WON'T SAY. IT'S A SECRET.

— The first sensible thing you've said all day — Gregory admitted.

— BUT I'LL GIVE YOU A CLUE: UNDER A FLOWERPOT!

Agnes closed her eyes.

— Please stop making everything easier, sir.

Announcement from the Golden Password Hotel: rooms now have separate locks, the vault has its own guard, and shouting “I'M THE MANAGER” is no longer accepted as an authentication method. A flowerpot audit revealed two keys, three password notes and an unpaid pizza bill. 🔑🏪🤣❤️