MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES

Liberté
Égalité
Fraternité

DIRECTION DES RESSOURCES HUMAINES

SOUS-DIRECTION DE L'ATTRACTIVITÉ ET DES RECRUTEMENTS

Bureau des concours et examens professionnels

Concours externe et interne pour le recrutement dans le grade de secrétaire des systèmes d'information et de communication de 2ème classe au titre de l'année 2025

Épreuve écrite d'admissibilité

8 janvier 2025

Anglais

Durée totale de l'épreuve : 1 heure – coefficient 2

Toute note inférieure à 8 sur 20 est éliminatoire

Traduction en français d'un texte à caractère technique rédigé en anglais

Ce sujet comporte 1 page (page de garde non comprise)

Passwords are giving way to better security methods – until those are hacked too

The Guardian, Sun 24 Nov 2024 (adapted text)

It's a war that will never end. But for small-business owners, it's all about managing risk while reaping rewards.

We humans are simply too dumb to use passwords. A recent study from password manager NordPass found that "secret" was the most commonly used password in 2024. That was followed by "123456" and "password". So let's all give praise that the password is dying.

Yes, we know that we should be using 20-letter passwords with weird symbols and numbers, but our minds can't cope. We use the same password for many accounts, be it for a newsletter subscription or our life savings. We all have too many passwords. So we opt for the easiest to remember – and steal.

Hackers know this and our passwords are available from the countless data breaches that occur on an almost daily basis on the dark web to anyone with a few bucks.

Now Mastercard, Visa and a whole host of other tech and finance firms are killing off passwords. Mastercard is aiming to end passwords and all that keying in of card details by 2030. Instead, biometric methods such as fingerprints or facial recognition will be used to see if it's the real you.

Microsoft, Apple, Google, Samsung and other big tech companies are moving towards what they call "passkeys". Under this security method, your pin is saved both on the cloud provider's site and on your device so that when you try to enter the site instead of using a password, you use the pin that's authenticated in both places, and as long as you're on the same device you're allowed access.

Until, of course, you lose that device or it gets stolen and the pin is hacked. Or a hacker uses a deepfake imitation of your voice to dupe an unsuspecting customer service with your stolen information. Or a hacker uses open-source software to hoax users into revealing their pin as they try to log in to a site. It happens. More than you would like to know. Or your biometric information is stolen through malware and then – using advanced AI with high-resolution photos or 3D imaging – replicated. This already happens.

Are rewards of technology greater than the risks of a data breach? For most small-business owners, the answer is yes.

Spoiler alert: even in a post-password universe, your company's data and your personal data are not safe. Tech companies will keep coming up with new ways to secure it, and hackers will find their way around. […]