Intitulé de l'épreuve : Anglais.

Nombre de copies :

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

les mots de passes sont abandonnés au profit de meilleures méthode de sécurité - jusqu'à ce qu'elles soient piratées elles aussi.
The Guardian, Dimanche 24 Novembre 2024.

C'est une guerre sans fin. Mais pour la patrons de petites entreprises il s'agit principalement d'une gestion des risques au détriment des gains.
Nous humains sommes trop stupides pour utiliser des mots de passe.
Une récente étude du gestionnaire de mot de passe Nordpass a indiqué que "secret" était le mot de passe le plus utilisé en 2024. Suivi de "123456" et "password". Alors prions tous pour que le mot le mot de passe disparaisse.

Oui, nous savons qu'il est nécessaire d'utiliser des mots de passe de 20 lettres, contenant des symboles et des chiffres, mais c'est trop contraignant pour nos esprits.
Nous utilisons le même mot de passe pour plusieurs comptes, que ce soit pour l'inscription à une revue de presse ou pour nos comptes en banque. Nous avons tous trop de mot de passe. Alors nous choisissons ce qui est plus facile à retenir - et à voler.

Les Hackers le savent et nos mots de passe sont disponible à cause d'innombrables fuites de données qui surviennent presque quotidiennement sur le Dark WEB pour quelques dollars.

Désormais Mastercard, Visa et bien d'autres ~~comp~~ entreprises de la finance et de la tech supprimerons le mot de passe.

N° ... /...

[redacted]

Mastercard a pour objectif de mettre fin aux mot de passe et tout ce système de cartes à puce dès 2030.
Au lieu de cela, des méthodes biométriques telles que la reconnaissance faciale ou l'empreinte digitale seront utilisées pour déterminer s'il s'agit bien de vous.

Microsoft, Apple, google, Samsung et beaucoup d'autres grosses entreprises de la tech penchent vers ce que l'on appelle des "pass'keys". Derrière cette méthode de sécurité, votre code PIN est sauvegardé sur le site du fournisseur de Cloud ainsi que sur votre appareil, de telle sorte que lorsque vous entrez sur le site, au lieu d'utiliser un mot de passe, vous utilisez le code PIN pour vous authentifier aux 2 endroits (site et appareil), tant que vous êtes sur le même appareil auquel vous avez autorisé l'accès.

A moins, bien sûr, que vous perdiez votre appareil ou bien qu'on vous le vole et qu'on pirate le PIN. Ou qu'un hacker utilise une imitation faite par intelligence artificielle de votre voix pour usurper votre identité et se faire passer pour vous auprès d'un service client crédule. Ou encore qu'un hacker utilise un logiciel open-source pour piéger les utilisateurs, les incitant à révéler leur PIN lorsqu'ils tentent de s'authentifier à un site. Cela arrive. Bien plus souvent que vous ne le pensez.
Vos données biométriques peuvent aussi être volées au travers d'un malware et les répliquer grâce à l'intelligence artificielle générant des photos à très haute résolution ou des images en 3D.

Est-ce que les gains qu'apporte la technologie sont plus importants que les risques? Pour la plupart des dirigeants de petites entreprises, la réponse est oui.

Alerte Spoiler : même dans un monde sans mot de passe, vos données personnelles et celle de votre entreprise ne sont pas en sécurité.

Les géants de la Tech trouveront de nouvelles méthodes de sécurité, et les hackers trouveront les moyens de les contourner.

N°
... /...

N°

... /...