Protecting Your Accounts and Devices

Common Guidance on Passwords

We believe that using stronger authentication is one of the most effective and inexpensive steps that can be taken to secure organizations and people online. On World More Than A Password Day, November 10, 2023, together we are issuing this Common Guidance on Passwords specifying simple steps that anyone can take to be more secure:

Steps to Take Now

1. **Use password-free authentication**
   Use password-free (passwordless) authentication, such as passkeys (sometimes other terms are used), when you can. Passkeys are simpler to use and far more secure than passwords. Passkeys use cryptography to prove that you are you for online sites and services, employing a secret key that is stored on your device and is never shared. The most popular operating systems, browsers, and email services support passkeys - just search for “passkey” and the name of your operating system, browser, or site/service.
2. **Secure your email account**
   If using password authentication for your email accounts, use a very strong password (long, randomly generated, and unique (see https://www.cisa.gov/sites/default/files/2023-08/Secure-Our-World-Passwords-Tip-Sheet.pdf) and multi-factor authentication/two-step verification (see the next step below). Email is the most common form of resetting your password, and you want to make sure no one else can “reset” your passwords and get access to your accounts.
3. **Add an extra layer of security above using passwords alone**
   Using a hardware security key or token, an authenticator app or a PIN provided by SMS messaging as a “second factor” in addition to your password can help prevent phishing and other attacks. This process can be called multi-factor authentication (MFA), two-factor authentication (2FA), or two-step verification. The better form of additional security is to use a hardware token or an authenticator app on your phone, and not to rely on SMS messages for the second factor.
4. **Use a password manager**
   Especially if you have accounts that use only a password and not passkeys or a second means of authentication, use a password manager so you don’t have to remember all your passwords. Using a password manager means you can use strong, randomly generated passwords that are much harder to guess. Software password managers, browsers that manage your passwords, and operating systems can all do a good job. Of course, your password manager password has to be both strong and memorable (see the next step to pick a good password), and you must respond quickly and change all your passwords if your password manager service is compromised. More detailed guidance on password managers is available, for example, from the

UK Password managers: using browsers and apps to safely store your passwords, and Canada Password managers-security.

5. **Use a recommended technique to pick passwords**
   If you are picking your own passwords rather than having your computer or password manager generate them, you can use a passphrase (Best practices for passphrases and passwords (ITSAP.30.032) - Canadian Centre for Cyber Security) or a technique like the UK NCSC's "Three Random Words" to pick passwords that are easier to remember but hard to guess. https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words.

If You are "Hacked"

6. **Changing passwords**
   Your passwords should be changed immediately if one of your devices is compromised (for example, a hacker installs malware on your computer). If an online site or service you use (an email service, a website, etc.) is hacked, change your password for that site or service and anywhere else you have reused that password (and you really should not reuse passwords). Subscribing to https://haveibeenpwned.com/ is a good way to discover if you have passwords you need to change. Last, it's best to change passwords using a device that hasn't been compromised.

   Note for providers: Require or support strong authentication rather than requiring that passwords be periodically changed.

Signed,

American University
Anti-Phishing Working Group (APWG)
Aspen Digital
Australian Cyber Collaboration Centre
Aviation ISAC
BBB Institute for Marketplace Trust
Bfore.Ai
Black Girls in Cyber
C3Initiative
Canadian Cyber Threat Exchange
Center for Democracy & Technology
Center for Internet Security
Center for Threat-Informed Defense
Charter of Trust
Cloud Security Alliance
Consumer Reports
Craig Newmark Philanthropies

CREST International
Cyber Defence Alliance
Cyber Threat Alliance
Cyber Readiness Institute
Cyber Risk Institute
Cyber Security & Forensics Association Uganda
CyberGreen Institute
CyberPeace Institute
Cybersecurity and Infrastructure Security Agency (CISA)
Cybersecurity Network Foundation
Cybersecurity Tech Accord
Cybertrust America
CyberWA, Inc
CyberWyoming Alliance
DECO PROTeste
Disarm Foundation
DNS Research Federation
Dominio PuntoGal
EURid
Euroconsumers
European Cyber Security Organisation (ECSO)
European Cybercrime Centre - EC3 - Europol
FIDO Alliance
Forge Institute
Forum of Incident Response and Security Teams (FIRST)
Get Safe Online
Girls Who Code
Global Anti-Scam Alliance
Global Cyber Alliance
Global Resilience Federation
Hacking the Workforce
Health-ISAC
HIKS
Institute for Security and Technology
Interpol
Kenya CyberSecurity & Forensics Association
Kosciuszko Institute
Maritime Safety & Security Alliance
Microsoft
National Council of ISACs
National Cyber Forensics and Training Alliance
National Cybersecurity Alliance

National Cybersecurity Society
Netsafe
Nomad Futurist
NSI Cyber and Tech Center, Antonin Scalia Law School at George Mason University
Open Cybersecurity Alliance
OWASP
Packet Clearing House
PUNTU.EUS
R Street Institute
Rapid7
Recorded Future
Retail & Hospitality ISAC
ScamAdviser
SecureThe Village
Security Scorecard
Serianu
Shadowserver Foundation
#ShareTheMicInCyber
Sightline Security
Society of Citizens Against Relationship Scams Inc.
South West Cyber Security Cluster
STOP. THINK. CONNECT. Messaging Convention
UC Berkeley Center for Long-Term Cybersecurity
Women4Cyber Foundation
XRSI
youthprotect e.V.

License