Personal Cybersecurity Checklist

Personal Cybersecurity Checklist

At Auth0 we care deeply about cybersecurity, and we want to help make the internet safer. Not only by increasing the security of your business through our platform, but also by spreading awareness about cybersecurity.

So we have prepared an easy checklist to help you, the people, and the kids you know, stay safe online. We believe in making cybersecurity accessible for everyone, so we've translated it to 9 languages with help from Auziros across the world.

Password Care and Maintenance

- I don't use the same password for different accounts.
- My passwords are at least 18 characters long whenever possible.
- I use a Password Manager like 1Password, LastPass, Keepass, or keychains supported by the operating system or browser.
- For accounts not in a password manager, I create long, unique and memorable passphrases.

Multi-factor Authentication (MFA)

- All my important accounts (email, social media, finance-related apps) are protected with Multi-Factor Authentication (MFA) through an app like Auth0 Guardian, Authy, Duo, Google Authenticator, or SMS if there's no other way.
- I save my MFA backup codes in a paper stored securely, or in my password manager.

You can find more information about MFA in our docs https://auth0.com/docs/multifactor-authentication

When NOT to click

- I avoid clicking on suspicious links, or downloading suspicious attachments from emails, or text messages I don't expect.
- I don't click on ads that promise free money, prizes, or discounts.
- We invite you to try out Google's Phishing Quiz https://phishingquiz.withgoogle.com/

Privacy

- I don't post private information like my home address, private pictures, phone number, or credit card numbers publicly on social media.
- I've configured my social media privacy settings to my preferences.
- I don't play with games, or answer surveys on social media that ask for sensitive private information.

You can find more information in our Privacy Guide, and the EFF https://auth0.com/blog/practical-privacy-a-guide-for-everyone/
https://www.eff.org/issues/privacy

Basic Cyber Hygiene

- I am cautious about the permissions I accept for all the apps I use
- I delete the applications that I no longer use
- I back up my important files.
- I have emergency contacts configured on my phone.
- I encrypt my phone, my computer, and my external hard drives
- I have configured https://haveibeenpwned.com/ to notify me in case my email appears on a breach.
- I keep the operating system of my computer and phone updated with the latest version at all times.
- I change the default passwords of my Internet of Things (IoT) devices.
- I keep my computer and phone locked with a password, or a pin longer than four numbers.
- I share information like this with friends and family to help them be safe.

Auth0, a global leader in Identity-as-a-Service (IDaaS), provides thousands of customers in every market sector with the only identity solution they need for their web, mobile, IoT, and internal applications. Its extensible platform seamlessly authenticates and secures more than 2.5 billion logins per month, making it loved by developers and trusted by global enterprises. The company's U.S. hea quarters in Bellevue, WA, and additional offices in Buenos Aires, London, Tokyo, and Sydney, support its global customers that are located in 70+ countries.

For more information, visit https://auth0.com or follow @auth0 on Twitter.

Cybersecurity best practices for kids

(ages 8+)

Sharing about me

• I only post pictures or videos of myself online if I have permission from my parents or guardians.

• If someone is asking me personal questions like my home address, where do I go to school, what's my phone number, or asking for pictures of me, I ask for help right away.

• I know that posting my name, birth date, home address, pictures, school address, phone number, or credit card numbers online can be dangerous for me and my family.

• I understand that in the online world, anyone can pretend to be someone they are not, so I shouldn't meet with them in person.

Safety Basics

• I only download or install applications when I have permission from my parents or guardians.

• I avoid using short and simple passwords like "test", "password", "123456" or "Charlie1"

• I use passwords consisting of words united by a dash (-) or a space. For example: ice-cream-chocolate-is-the-best

• My passwords don't include my name, birth-date, pet's name, or other information that can be guessed.

• All my accounts use different passwords.
I don't click on pictures that promise free money, prizes, or games.

Keeping it kind (for myself and others)

• I know that I may not be able to delete things I post online, and others can copy/repost them. It could even be connected to me 20 years from now.

• I ask for help if someone says something hurtful to me online. I also report, and block them if I can.

• I mostly ignore comments, but if they get too scary, I report them.

• I treat others with kindness online, just like I would treat them in person.

• How I feel about myself doesn't depend on other people's likes or comments on social media.

auth0.com