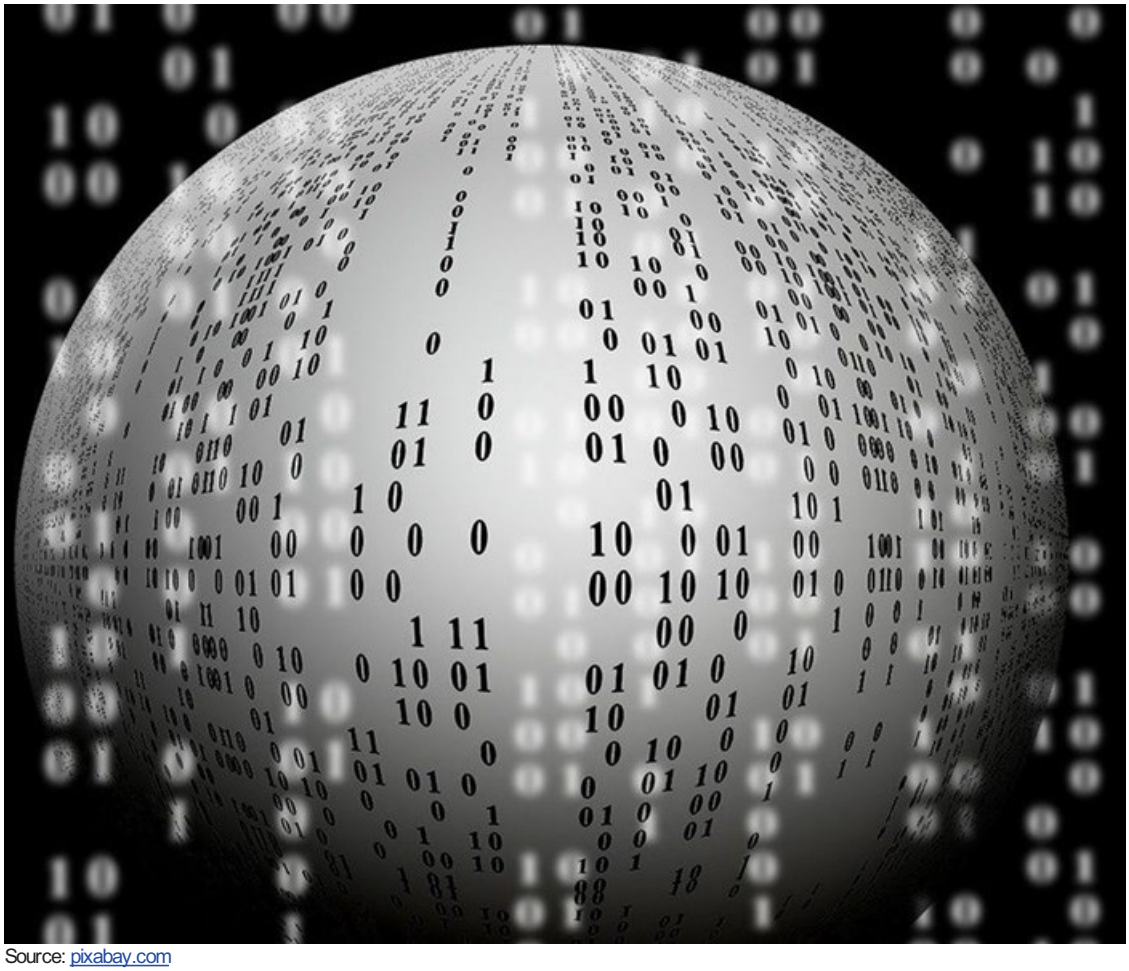
BIZCOMMUNITY

6 online privacy tips for everyone

28 January was Data Privacy Day and NordVPN is issuing a reminder about simple online privacy rules that everyone should follow to stay safe and secure.



Source: pixabay.com

“We are glad that Data Privacy Day exists,” says Ruby Gonzalez, head of communications at NordVPN. “However, Privacy Day should be every day. There are simple things that are easy to maintain every day in order to avoid major hacks, system crashes, data loss and various snoopers.”

NordVPN shared main online privacy rules for everyday internet user:

1. Always update the software

Software manufacturers constantly find new bugs and fix them with each new update, but users need to keep their systems up to date. Bugged software might cause data leaks, putting user’s privacy at risk.

2. Be cautious about what you share on social media

Have in mind that what you post online, stays online. If you are going on vacation, it’s wiser to post vacation photos after you come back – otherwise, thieves might know your house is empty. Also, don’t share any personal details, addresses or phone numbers.

3. Switch to an encrypted email provider

ProtonMail is an example of a free encrypted email service provider, offering end-to-end encryption – meaning even the provider itself cannot decrypt and read subscribers' emails. No personal information is required to create accounts, and the basic account service is offered free of charge. Other secure email providers include Tutanota and Countermail.

4. Use strong passwords and a password manager

Perhaps the most basic requirement for any online account setup is using strong passwords and choosing different passwords for different accounts. Weak passwords make it simple for hackers to break into an account. A reliable password has a minimum of 12 characters and includes a strong mix of letters, numbers and characters. It's not easy to remember strong passwords for each site, so it's recommended to use a password manager, though some – such as LastPass – have also experienced security breaches. In any case, password managers are still recommended for safety and security – such as truekey.com and 1Password.

5. Turn on multi-factor authentication

Multi-factor authentication is a security system that requires a user to log in with their username and password and then take the second step of authentication: either through a fingerprint scan or by sending a code via text. Most sites, including email providers, already offer multi-factor authentication as an option.

6. Use a VPN

A VPN encrypts all traffic between a user's computer and a VPN server, adding privacy and security to their Internet browsing experience. The only information visible to anyone in between the user's computer and VPN server is the fact they are connected to VPN – and nothing else. All other information is private as it is encrypted by the VPN's security protocol. NordVPN secures users' data with features like automatic kill switch and a strict no logs policy.