7 Cybersecurity predictions for 2023

A digital privacy expert forecasts what cybersecurity will look like next year

In 2022, governments fought wars online, businesses were affected by multiple ransomware gangs, and regular users' data was constantly on hackers' radar.

Marijus Briedis, CTO (chief technical officer) of NordVPN, says, "Next year will not be any easier when it comes to keeping users' data safe and private. Authoritarian countries and hackers are working hard to compromise those factors. However, I see the light at the end of the tunnel because people are starting to value their data, pushing businesses and governments to take action."

Every year, digital privacy experts at NordVPN assess cybersecurity trends — these are the top seven that made the New Year's security prediction list.

- **5G will create more cybersecurity challenges.** New technology always comes with a risk that hackers will find ways to exploit it. Even though 5G will provide users with a faster internet connection, it will also require significant attention to be paid to the new infrastructure, opening more access points for hackers to compromise. And with the global shortage of cybersecurity experts, it will be increasingly difficult to prevent that.

- **Bye-bye, third-party cookies.** Google promised to eliminate third-party cookies in Chrome browsers by 2024. This is great news for anyone who values their privacy. Third-party cookies are trackers that collect individual user data across countless websites, which end up in advertisers' hands to create personalized and intrusive ads. At the moment, Google is thinking of new ways to track its flow (such as through FLoC). So even though we cannot say that user tracking is gone, we can celebrate the era of intrusive tracking coming to an end.

- **2023 will be a big year for privacy laws.** In January 2023, India will discuss its Personal Data Protection Bill — the Indian version of the GDPR. Similarly, the US may be discussing its own American Data Privacy and Protection Act, which will help establish a framework for data protection at the federal level.

- **Authoritarian states will further isolate their citizens from the WWW.** Countries like Iran, Russia, and China are consolidating their power to increase surveillance by government actors. So even though many countries are fighting for democracy, the actions of those states will keep their citizens in the dark.

- **The cyberwar is only starting.** With China's leader securing his third term and Russia's war in Ukraine, many experts predict an increase in state-sponsored cyberattacks. China may increase cyberattacks on Taiwan, Hong Kong, and other countries opposing the regime. Meanwhile, Russia is predicted to sponsor attacks on countries supporting Ukraine.

- **Next era of encryption.** In the face of quantum computing power even the most sophisticated encryption algorithms can be broken in a couple of minutes. This shows that in the future new and more powerful encryption tools will be needed.

- **Cybersecurity will become blockchain-based.** Blockchain has proven extremely useful for secure and decentralized information exchange. Up until now, blockchain-based tools have been too expensive to implement because of the novelty of the technology. However, many experts predict that in 2023 blockchain technology will be used in cybersecurity more and more often.

ABOUT NORDVPN

NordVPN is the world's most advanced VPN service provider, used by millions of internet users worldwide. NordVPN provides double VPN encryption and Onion Over VPN and guarantees privacy with zero tracking. One of the key features of the product is Threat Protection, which blocks malicious websites, malware, trackers, and ads. NordVPN is very user friendly, offers one of the best prices on the market, and has over 5,000 servers in 60 countries worldwide. For more information: nordvpn.com