BIZCOMMUNITY

NordVPN's 5 cybersecurity predictions for 2019

Cybersecurity threats will keep getting worse in 2019.

It's not an easy task to remember a week in 2018 without a major data leak or security breach. Passwords were leaking, new sophisticated malware attacks were spreading, data was breached, and governments around the world once again overturned privacy rules.

NordVPN's digital privacy expert, Daniel Markuson says that 2019 will keep getting worse.

Daniel Markuson, digital privacy expert at NordVPN

> *"The year 2018 not only (yet again) shocked the world by highlighting systemic cybersecurity issues. Multiple governments adopted newrules and laws, which are making a global impact nowand will echo for years to come,""Still, 2019 can bring some hope for the future – but only if governments and corporations understand the importance of digital privacy and security."*

Based on the outcomes from 2018, Markuson lists five significant trends that will shape cybersecurity and digital privacy in 2019:

1. Identity theft, phishing scams, and personal data loss will hit a new high

From Facebook and Google to Quora and Marriott, last year's data breaches have affected more than one billion people around the globe. Add that to the existing pool of leaked data, and hackers will have an invaluable resource for tailoring a phishing scam or taking over your Facebook or Netflix account. Without a doubt, it will be used in 2019.

2. Some governments will lean towards higher data security standards

The GDPR in the EU established a new set of game rules by regulating the way corporations protect the data of their customers. It is still early to tell whether the new regulations have made a positive impact, but they have brought a shift towards more responsible use of private data.

In 2019, some non-EU countries will likely follow the example and introduce a similar set of laws for data protection as well. This year, all eyes will be on the US, where California has set a high bar by passing the Consumer Privacy Act. However, it is still unclear if other states will follow. We really hope they do!

3. Use of encrypted communications will face new challenges

In December 2018, Australia passed the Assistance and Access (A&A) bill, also known as anti-encryption law – all despite an uproar within the society. The bill requires tech companies to create backdoor access to the encrypted communications of their users. It would be used by law enforcement agencies to intercept and read the content of the private messages.

Despite the opposition to the law, similar ideas have been floated in multiple countries including the US. Having in mind the everlasting itch to spy on their citizens, it wouldn't be a shocking surprise if other members of the '14-eyes' countries would follow this example in 2019.

4. Tech companies will look for new ways to win the trust of their potential customers

A lot of data has been stolen this year. Despite the companies' size and significance, despite the self-proclaimed 'best security practices,' despite the risk of being fined under the GDPR. It's no surprise that ensuring customers' trust will become more critical than ever. Companies will learn (although slowly) from their mistakes and invest in penetration testing, security audits, AI, and implementing zero-trust policies to prove that they are making an effort to protect their clients.

5. Cloud security will become a bigger issue

As people change locations and devices, cloud computing becomes inevitable both for private users and corporations. At the same time, it becomes a bigger security problem. GoDaddy, Los Angeles 211 center, Viacom, and just recently the United Nations had their data records harvested from cloud storage. The biggest issue is still simple configuration errors and user neglect.

Nevertheless, as we can expect more leaks and breaches here, new cloud security measures and services will come out in 2019.