Grant Thornton

Cybersecurity Cases Widely Discussed on Social Media in 2023

January 2024

Cybersecurity Cases Widely Discussed on Social Media in 2023

The widespread development of digital technology requires society today to be more adaptive to the information received. The rapid dissemination of news, easy access to learning resources, and the convenience of online shopping are real examples of the positive aspects of digital development.

Despite the positive aspects, there are also negative effects that require people to be more cautious about digital development. The prevalence of hoaxes, misinformation, violations of the Information and Electronic Transactions Law (UU ITE) against certain groups, and the cyberattacks that went viral in Indonesia during the past year are examples of dangers of the rapid development in technology, which have often become hot topics on social media.

Do you know the viral cybersecurity cases that were widely discussed in 2023? Here are some of them:

Phishing is online fraud conducted through fake emails, links, websites, or phone calls designed to closely resemble the real ones. The goal of phishing is to obtain sensitive data and information, such as bank account details, usernames, or passwords. Have you heard of the phishing cases that use fake wedding invitations to lead people to an Android Package Kit (APK) document? The messages are sent in the form of APK files to victims who are forced to click or open the APK file and download it to their phones or PCs, allowing the virus to be installed. This phishing method usually exploits the users' ignorance in sharing their personal information.

Ransomware is a type of malicious program or malware that threatens victims by destroying or blocking access to important data or systems until the victims have paid for the data. One major ransomware case that shocked Indonesia in 2023 was the paralysis of Bank Syariah Indonesia's (BSI) services which included their online banking and automated teller machines (ATMs) for some time. This case was driven by a cyber gang called Lockbit that threatened to leak the data if a ransom was not paid.

Last year, there were some cases of **data leaks** involving government offices such as the civil registration and population administration data (Data dukcapil), the voters' list data (data DPT KPU), and the sale of Indonesian passport data for $10,000 USD on the dark web. Because of these cases, the Ministry of Communication, and Information Technology (KOMINFO) collaborated with the National Cyber and Crypto Agency (BSSN) to investigate the causes of these incidents.

The rapid development of technology in this era of digitization has undoubtedly led to the development of tactics and strategies for digital criminals. It is time for us, as users, to be more aware of and vigilant towards our actions in the digital world. You can start by keeping your ATM PINs private, constantly changing your account passwords, and avoiding the download of applications or documents from untrusted sites. Lastly, cybercrimes can infiltrate your systems from anywhere and target individuals or groups, so do not forget to use your technology wisely.

Written by:

Kaifa Raihana Fatah
Associate Consultant
IT Advisory

grantthornton.co.id

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton International Ltd (GTIL) and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.