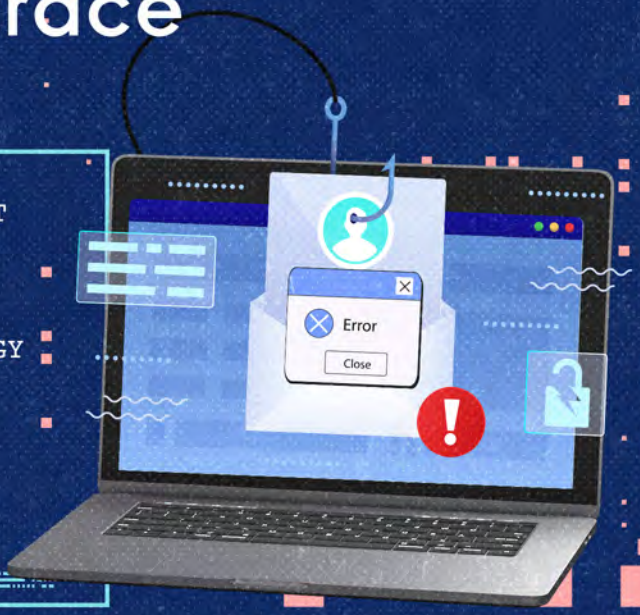
hacktrace

INDONESIA HAS EXPERIENCED A SIGNIFICANT RISE IN DATA BREACHES IN RECENT YEARS. ACCORDING TO A REPORT BY THE COMMUNICATION AND INFORMATION TECHNOLOGY MINISTRY (KOMINFO), THERE WERE **15 MILLION** DATA BREACHES RECORDED IN INDONESIA IN 2022.



THE MOST COMMON TYPES OF DATA BREACHES IN INDONESIA ARE:

PHISHING ATTACKS

These attacks involve tricking victims into clicking on malicious links or opening attachments that contain malware.

SOCIAL ENGINEERING ATTACKS

These attacks involve installing malware on a victim's computer or device without their knowledge. Malware can steal data, damage files, or take control of a computer.

MALWARE ATTACKS

These attacks involve tricking victims into revealing personal information or clicking on malicious links.

THE CONSEQUENCES OF DATA BREACHES CAN BE SEVERE, INCLUDING:

- FINANCIAL LOSSES
- DAMAGE TO REPUTATION
- LEGAL LIABILITY

TO PROTECT THEMSELVES FROM DATA BREACHES, INDONESIAN BUSINESSES SHOULD TAKE STEPS TO:

RAISE EMPLOYEE AWARENESS OF CYBERSECURITY RISKS

Employees should be trained on how to identify and avoid phishing attacks, malware attacks, and social engineering attacks.

IMPLEMENT STRONG CYBERSECURITY CONTROLS

Businesses should implement strong cybersecurity controls, such as firewalls, intrusion detection systems, and data encryption.

HAVE A DATA BREACH RESPONSE PLAN

Businesses should have a data breach response plan in place to help them quickly and effectively respond to a data breach.

www.hacktrace.id

hacktrace

CYBERSECURITY AWARENESS TRAINING

PROTECT YOUR ORGANIZATION FROM CYBER THREATS

WHAT IS CYBERSECURITY AWARENESS TRAINING?

Cybersecurity awareness training is a type of training that helps employees understand and mitigate cybersecurity risks. This type of training can help to reduce the risk of data breaches, identity theft, and other cyberattacks.

CYBERSECURITY AWARENESS TRAINING SHOULD COVER A VARIETY OF TOPICS, INCLUDING:

SOCIAL ENGINEERING

This type of attack involves tricking employees into revealing personal information or clicking on malicious links.

PHISHING

Phishing emails are designed to look like they are from a legitimate source, such as a bank or credit card company.

MALWARE

Malware is malicious software that can be installed on a computer without the user's knowledge. Malware can steal data, damage files, or take control of a computer.

PASSWORD SECURITY

This type of attack involves tricking employees into revealing personal information or clicking on malicious links.

BENEFITS OF CYBERSECURITY AWARENESS TRAINING

There are many benefits to cybersecurity awareness training, including:

- Reduced risk of data breaches, identity theft, and other cyberattacks
- Increased employee understanding of cybersecurity risks
- Improved employee cybersecurity behavior
- Reduced costs associated with cyberattacks

www.hacktrace.id