

Cybersecurity

Why is Cybersecurity Important?

Cybersecurity is crucial to a business for a myriad of reasons. The two this section will focus on are data security breaches and sabotage. Both can have dire effects on a company and/or its clients.

Data security breaches can compromise secure information such as:

- Names and social security numbers
- Credit card and bank details
- Trade secrets
- Intellectual property

Computer sabotage serves to disable a company's computers or network to impede the company's ability to conduct business.

Phishing

Cybercriminals who use phishing scams aim to obtain personal information by appearing to be a legitimate source. Many times, they masquerade as a major company, such as a bank, appealing to your desire to keep your information safe.

For example, they may send an email that says, "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

Clicking the link or responding to the email can take you to a website that looks authentic, but is in fact a spoof site that serves to steal your information and use it for malicious purposes, such as commit crimes using your name or using your bank information for personal gain.



Cryptography

Cryptography is basically defined as a secret method of writing. This is done so that only authorized parties are able to interpret the message.

It is used in various industries, such as banking and health to protect the privacy and security of companies and customers'/patients' information.

Examples of encryption methods include:

- International Data Encryption Method (IDEA)
- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)