ONE PAGE SUMMARY

IT & Software › Cyber Security › Cyber Security Basics

Introduction to Cyber Security Basics

Master the essentials of Cyber Security to protect your digital life.

DEFINITION

> Cyber security involves protecting computer systems and networks from digital attacks and unauthorized access. It ensures the confidentiality, integrity, and availability of information.

KEY CONCEPTS

Confidentiality

Ensures that sensitive information is accessed only by authorized users.

Integrity

Maintains the accuracy and trustworthiness of data over its lifecycle.

Availability

Ensures that information and resources are accessible to authorized users when needed.

Threats

Potential dangers that can exploit vulnerabilities, such as malware or phishing attacks.

Vulnerabilities

Weaknesses in a system that can be exploited by threats to gain unauthorized access.

EXAMPLES

→ Using strong, unique passwords for different accounts.

→ Installing antivirus software to detect and remove malware.

→ Regularly updating software to patch security vulnerabilities.

MEMORY TIPS

★ Remember C-I-A: Confidentiality, Integrity, Availability.

★ Think of threats as 'bad guys' and vulnerabilities as 'open doors'.

★ Use the acronym P.A.C.E. for prevention: Protect, Assess, Control, Educate.

COMMON MISTAKES

✗ Ignoring software updates and patches.

✗ Using the same password across multiple sites.

✗ Underestimating the importance of data backups.

QUICK RECAP

Cyber security is crucial for protecting information from unauthorized access and attacks. Focus on the C-I-A triad: Confidentiality, Integrity, and Availability, and be aware of threats and vulnerabilities to enhance your security posture.