"Let your plans be dark and impenetrable as night..."

Sun Tzu, The Art of War

THE ART OF CYBER WAR

PASSWORD SECURITY

81% of hacking-related breaches leveraged either stolen and/or weak passwords (Data Breach Investigations Report, 10th Edition, Verizon).

If you fail to protect your password or choose a weak password, you are at risk. A weak password can be guessed by hackers in minutes. A strong (long and complex) password made of uncommon words, lowercase letters, uppercase letters, numbers and symbols, could take weeks or months for a hacker to crack!

- Good Password: 8HR9@3d%uL#W
- Bad Password: Password1

If you suspect your account has been compromised, change your password immediately and contact your system administrator.

Our security awareness program will bring you up-to-speed on important cyber security topics through engaging training modules and simulations. In the coming weeks and months, you'll learn how to spot phishing attempts and other cyber threats before they occur, helping keep your organization's sensitive information safe.

PASSWORDS: BEST PRACTICES

Pick strong, complex passwords that are hard to guess

Use password storage applications with encryption

Keep your passwords private at all times

Change your passwords regularly

SecurityIQ
BY INFOSEC INSTITUTE

YOUR PASSWORD IS A TARGET.

81% of hacking-related breaches leveraged either stolen and/or weak passwords (Data Breach Investigations Report, 10th Edition, Verizon).

If you fail to protect your password or choose a weak password, you are at risk. A weak password can be guessed by hackers in minutes. A strong (long and complex) password made of uncommon words, lowercase letters, uppercase letters, numbers and symbols, could take weeks or months for a hacker to crack!

- Good Password: 8HR9@3d%uL#W
- Bad Password: Password1

If you suspect your account has been compromised, change your password immediately and contact your system administrator.

Our security awareness program will bring you up-to-speed on important cyber security topics through engaging training modules and simulations. In the coming weeks and months, you'll learn how to spot phishing attempts and other cyber threats before they occur, helping keep your organization's sensitive information safe.

SecurityIQ
BY INFOSEC INSTITUTE

PASSWORDS: BEST PRACTICES

Pick strong, complex passwords that are hard to guess

Use password storage applications with encryption

Keep your passwords private at all times

Change your passwords regularly

"If you know the enemy and know yourself, you need not fear the result of a hundred battles..."

Sun Tzu, The Art of War

THE ART OF CYBER WAR

RANSOMWARE ATTACKS

According to a recent Verizon research report, ransomware is the fifth most common type of malware, extorting millions of dollars from people and organizations after infecting and encrypting their systems (Data Breach Investigations Report, 10th Edition).

Ransomware holds hostage technology and data that is critical for running your most vital operations. Ransomware locks technology and demands money to regain access.

Our security awareness program will bring you up-to-speed on important cyber security topics through engaging training modules and simulations. In the coming weeks and months, you'll learn how to spot phishing attempts and other cyber threats before they occur, helping keep your organization's sensitive information safe.

AVOIDING RANSOMWARE: BEST PRACTICES

Use antivirus, file inspection and updates to avoid infection

Make regular backups and isolate backups from the rest of the system

If ransomware strikes, get help immediately and restore system from isolated backups

Don't pay ransom demands and get advice from law enforcement

SecurityIQ
BY INFOSEC INSTITUTE

YOUR TECHNOLOGY IS A TARGET.

According to a recent Verizon research report, ransomware is the fifth most common type of malware, extorting millions of dollars from people and organizations after infecting and encrypting their systems (Data Breach Investigations Report, 10th Edition).

Ransomware holds hostage technology and data that is critical for running your most vital operations. Ransomware locks technology and demands money to regain access.

Our security awareness program will bring you up-to-speed on important cyber security topics through engaging training modules and simulations. In the coming weeks and months, you'll learn how to spot phishing attempts and other cyber threats before they occur, helping keep your organization's sensitive information safe.

AVOIDING RANSOMWARE: BEST PRACTICES

Use antivirus, file inspection and updates to avoid infection

Make regular backups and isolate backups from the rest of the system

If ransomware strikes, get help immediately and restore system from isolated backups

Don't pay ransom demands and get advice from law enforcement

SecurityIQ
BY INFOSEC INSTITUTE