QUALIZEAL

Top 5

CYBER THREATS

And How To Prevent Them

Phishing Attacks

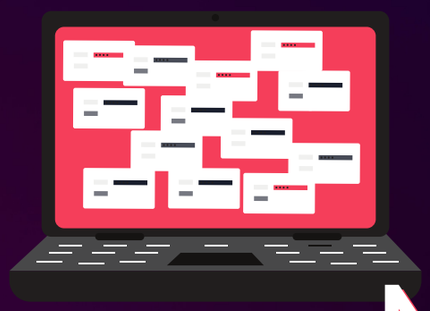
Phishing Attacks Are A Type Of Social Engineering Attack That Trick People Into Revealing Sensitive Information, Such As Login Credentials, Credit Card Numbers, Or Other Sensitive Information. To Prevent Phishing Attacks, It's Important To Educate Employees About The Dangers Of Phishing, To Use Two-Factor Authentication, And To Install Anti-Virus And Anti-Malware Software.

Ransomware Attacks

Ransomware Attacks Are A Type Of Malware That Encrypts A Victim’s Files And Demands A Ransom Payment In Exchange For The Decryption Key. To Prevent Ransomware Attacks, It’s Important To Backup Important Data, To Keep Software And Systems Up To Date, And To Use Anti-Virus And Anti-Malware Software.

Malicious Software (Malware)

Malware Is Any Software That Is Designed To Harm Or Exploit A Computer Or Network. To Prevent Malware Infections, It's Important To Keep Software And Systems Up To Date, To Use Anti-Virus And Anti-Malware Software, And To Avoid Downloading Attachments Or Visiting Websites From Untrusted Sources.



Network Intrusions

Network Intrusions Are Unauthorized Access To A Computer Or Network. To Prevent Network Intrusions, It’s Important To Use Strong Passwords, To Keep Software And Systems Up To Date, And To Use Firewalls, Intrusion Detection And Prevention Systems, And Network Segmentation.

Insider Threats

Insider Threats Are A Type Of Security Breach That Involves Individuals With Authorized Access To A Computer Or Network. To Prevent Insider Threats, It's Important To Implement Access Controls And Privilege Management, To Monitor Network Activity, And To Educate Employees About Security Best Practices.