

TECH. TUESDAY

HOLIDAY PHISHING

What is Phishing? Phishing is the fraudulent attempt to obtain sensitive information such as passwords or credit card details by tricking a person(s) to performing an action such as clicking a link or downloading a file. Phishing occurs primarily through email but can also occur through text messaging (smishing), voice calls (vishing), QR Codes (Qrishing) or compromised websites.

How can you protect yourself from this?

THE REAL COST OF A PHISHING ATTACK

- Lost working hours from employees
- Remediation
- Incident response
- Damaged reputation (to potential or current customers)
- Lost intellectual property
- Direct monetary losses
- Compliance fines
- Lost revenue
- Legal fees



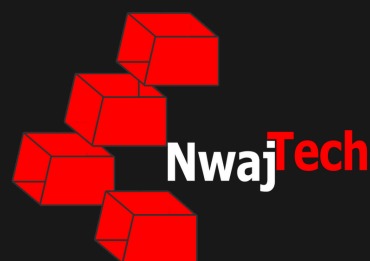
HOW CAN YOU RECOGNIZE A PHISHING ATTACK?



- Legitimate companies don't ask for sensitive info via email
- Attackers play on emotions, primarily fear
- It states "Suspicious Activity" or "A Problem with Your Account"
- Poor Grammar
- Fake links (Hover over the link to verify what you are clicking on)
- They don't use your name
- Email doesn't match company name

THE BEST DEFENSE IS A STRONG OFFENSE

- Education is Key
- Don't click questionable links, manually navigate to a site
- Verify the sender via phone/text before downloading
- Phishing mitigation software
- Ensure the site you're shopping on is secure and reputable
- Phishing Simulation
- DMARC, DKIM, SPF Records
- Breach Monitoring
- Stay Up To Date
- Review Statements
- Use Complex Passwords and MFAs (Multi-factor authentication)
- Privacy.com



@NwajTech
@MidstateCoC



@NwajTech
@MidstateCoC



www.nwajtech.com
www.midstatechamber.com