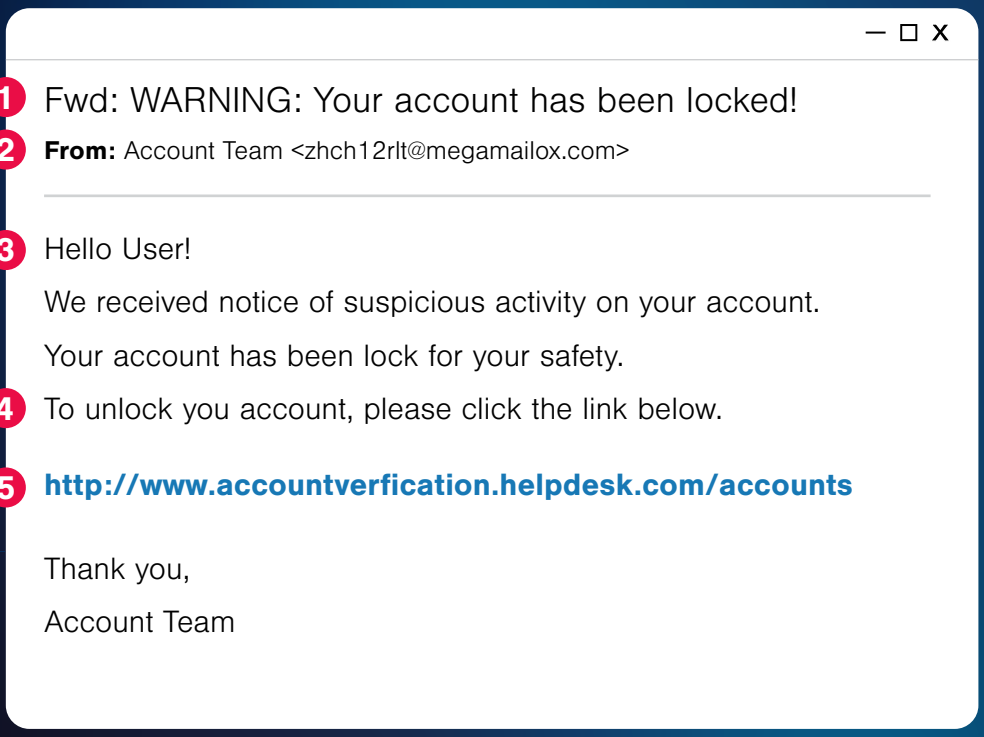
Phishing

What You Need To Know

What is Phishing?

Phishing is a cybercrime in which a threat attacker falsely impersonates a legitimate business or sender to lure victims into sharing personal or sensitive information. Phishing attacks often use email spoofing techniques designed to trick victims by asking them to update or verify their personal information by replying to the email or visiting a website. Spoofed websites might look nearly identical to the real thing–like your bank or credit card site–and ask the user to enter sensitive information like passwords, credit card numbers, banking PINs, etc. These fake websites are used solely to steal your information.

SIGNS OF EMAIL PHISHING



1. **SUBJECT LINE** – Sense of urgency or alarm
2. **SENDER** – Legitimate sender you deem trustworthy
3. **GREETING** – Non-personalize, generic greeting
4. **CLOSING REQUEST** – A call for immediate action
5. **HYPERLINK** – Statement requesting you link

PHISHING STATISTICS

96% of phishing attacks arrive by email

76% of U.S. organizations have experienced a phishing attack

30% of phishing emails are opened

80% of reported security incidents were phishing attacks in 2022

1.5 Million new phishing sites are created everyday

ATSG

If you suspect you have been the victim of a phishing attack, report the incident immediately to Security. If you believe an email is a phishing scam, contact the IT Department. Do not click any 3rd party links.