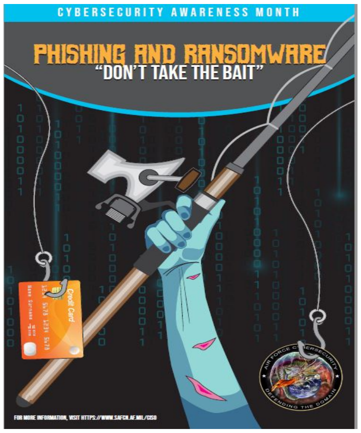
Air Mobility Command
Cybersecurity Awareness Month
Newsletter

11 October 2021 Vol II Issue II

CYBERSECURITY AWARENESS MONTH

Do Your Part. #BeCyberSmart

Week 2: Phishing & Ransomware



For more information contact your Wing CyberSecurity Office or e-mail the HQ AMC Cybersecurity Office at AMC.Cybersecurity@us.af.mil

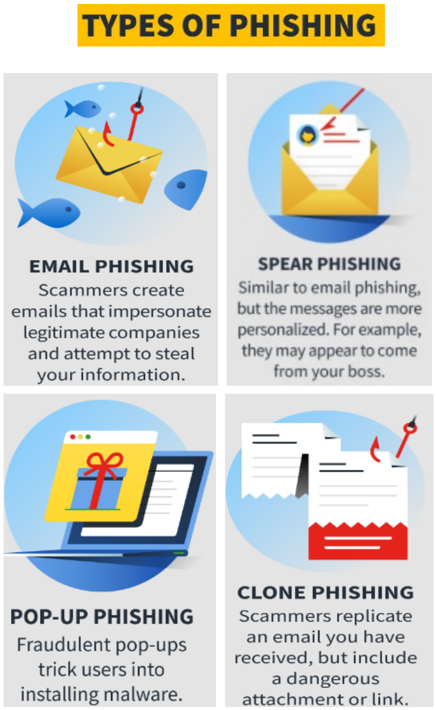
Tips & Guidance

Cyber hygiene habits keep networks healthy

When in doubt, report attacks

Regular data backups makes easier recovery

Keep calm & patch on



TYPES OF PHISHING

EMAIL PHISHING
Scammers create emails that impersonate legitimate companies and attempt to steal your information.

SPEAR PHISHING
Similar to email phishing, but the messages are more personalized. For example, they may appear to come from your boss.

POP-UP PHISHING
Fraudulent pop-ups trick users into installing malware.

CLONE PHISHING
Scammers replicate an email you have received, but include a dangerous attachment or link.

Phishing

The human factor is the weakest link in the security chain. Attackers persuade and deceive employees in many ways to gain access but one method stands out in its scale: **email.**

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons like executing and propagating malicious content disguised as a trustworthy entity in electronic communication.

Spear phishing is a more sophisticated type of phishing. Threat actors gather information on key people in an organization to provide confidential information or deliver certain malicious content, i.e. ransomware delivery and silent malware.

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand a ransom in exchange for decryption. These actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the nation, state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Recent attacks on the water we drink, our food production, healthcare availability, schools, municipalities, and other national critical infrastructures have demonstrated cyberattacks against key frameworks can have a significant impact on critical functions of government and private sector. All organizations should implement an **effective cybersecurity program** to protect against cyber threats and manage cyber risk commensurate especially organizations that deal with national security, national economic security, and/or national public health and safety.

Ransomware attacks are estimated to cost $6 trillion annually by end of 2021. https://www.cisa.gov/stopransomware/ransomware-101

CSAM Virtual Events and other resources are available at:

https://www.safcn.af.mil/Organizations/CISO-Homepage/Cybersecurity-Awareness-Month-CSAM/CSAM-2021/

External Link Disclaimer Policy: The appearance of hyperlinks does not constitute endorsement by the United States Air Force, or the Department of Defense, of the external Web site, or the information, products or services contained therein. References to non-federal entities do not constitute or imply Department of Defense or Air Force endorsement of any company or organization.