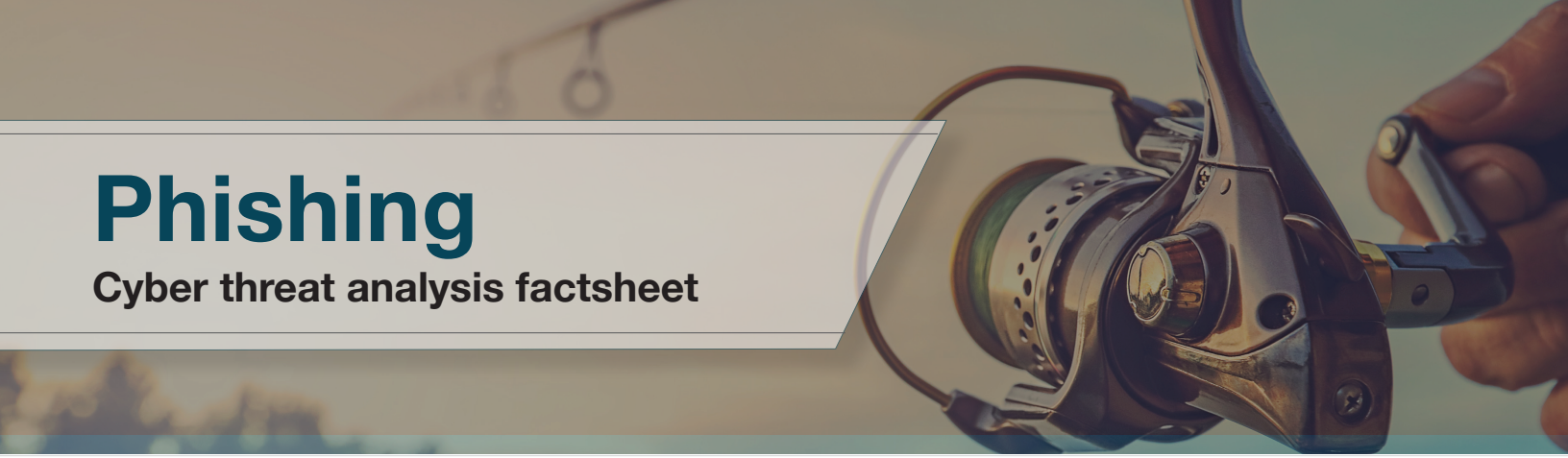

Phishing

Cyber threat analysis factsheet

What is phishing?

Phishing is the intentional attempt to obtain personal credentials or personally identifiable information (PII) by electronic communications (emails, text messages, and phone calls) that appear legitimate with links or attachments that may enable malicious software. These emails often request verification of sensitive information or request passwords are reset, with warnings of serious consequences if action is not taken quickly.

Current trend:

Microsoft phishing email campaign

This trending phishing attack targets Microsoft user credentials. Numerous government agencies have been targeted, and anyone can easily become a victim. A phishing email claims to be from Microsoft and requests the user to reset an expired Microsoft password.

The email looks legitimate and includes a URL to link to a spoofed Microsoft screen. This screen appears authentic, but steals the user's credentials, if the user completes the reset action. Once the credentials are stolen, users are redirected to a legitimate Microsoft website, while attackers begin performing malicious behavior using the stolen credentials.

Identify phishing emails

Phishing emails are disguised to look like legitimate emails, but often have characteristics that signal a scam. See Figure 1 for an example of phishing email characteristics, which may include a combination of the following:

- Suspicious URLs and/or Attachments
- Unnecessary urgency
- Unsolicited emails and/or suspicious sender
- Requests for personal or sensitive information, including passwords, Personal Identification Numbers (PINs), or bank account information
- Incentives, such a cash reward or payment, or threats, such as suspension of an account
- Business branding (e.g., the Microsoft logo) that appears legitimate, including copyrights intended to look official
- Omission of your name, or usage of a part of your name you do not typically use
- Misspellings or incorrect grammar

The Impact of a Successful Phishing Campaign

Aside from stolen credentials or installing malware, when employees fall victim to a phishing attack, intellectual property theft can be the most devastating loss of all. Mission critical data, technological enhancements, or research supporting military programs or our legal and justice system can all be compromised by successful phishing attempts.

U.S. Department of Justice
Office of the Chief Information Officer

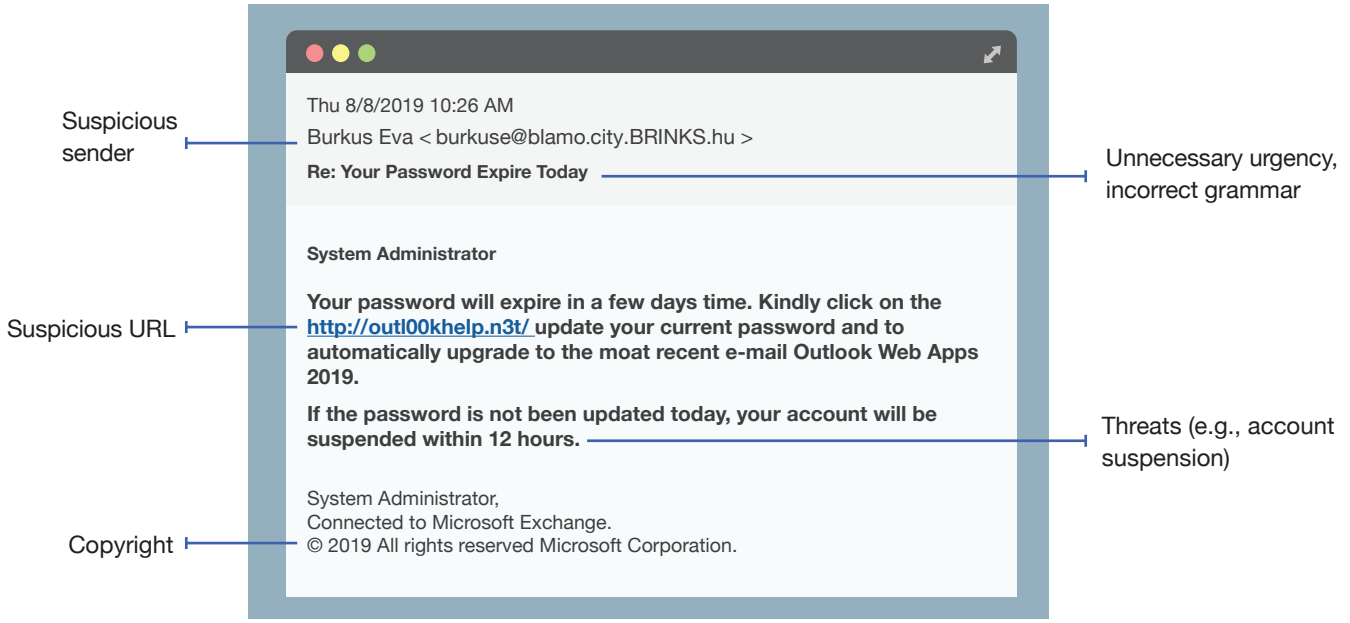

Figure 1: Example of phishing email characteristics
Note: email address and URL above are fictitious

Protect yourself and your colleagues

Phishing emails are now more sophisticated, more realistic-looking, and more challenging to recognize. Take steps to protect yourself and the federal government:

- Always use discretion—lookout for suspicious or unsolicited emails, text messages, and phone calls.
- Carefully examine URLs—hover over links to see the embedded URLs.
- Never provide sensitive personal information via websites, email, or by phone—unless secure.
- Only open email attachments you are expecting and know what is contained—open Zip files with caution because malicious content may be enclosed.

DOJ Cybersecurity Services

To help other government agencies strengthen their cyber defenses, DOJ provides a holistic security service including Security Operations Center, Trusted Internet Connection (TIC), continuous monitoring, and an unmatched capability to integrate cyber intelligence across the federal government.

Let us worry about security so you can focus on your mission.

To learn more, visit Justice.gov.

Report phishing emails

Immediately report any suspicious email to your system administrator or your Security Operations Center.

U.S. Department of Justice
Office of the Chief Information Officer

OWN SECURE PROTECT IT. OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart