H E A D Q U A R T E R S
CYBER COMMAND, ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN 2026-03

Preventing Security Breaches Caused by Malicious Links and Attachments

Overview

Cybercriminals are actively distributing emails, messages, and links that appear to come from trusted organizations, banks, or known contacts. These messages often contain attachments or links that, once opened, can install malware or redirect users to fake websites designed to steal login credentials and financial information.

Because these messages appear legitimate and are often contextually relevant, they can bypass security systems and exploit human trust.

What is Happening?

Cybercriminals commonly exploit malicious links and attachments as an easy way to infiltrate unsuspecting users' devices and networks. They often disguise these threats within legitimate-looking emails, messages, or websites, making them appear trustworthy and harmless.

These links or attachments may look like invoices, job, offers, or urgent security alerts, tricking individuals into clicking or downloading them. Once opened, hidden malware can be installed on the device, enabling attackers to steal sensitive information such as passwords and financial data, monitor user activity, or even gain full control of the system.

Most of the attacks rely on creating a sense of urgency or fear, causing users to act quickly without verifying the source. As a result, cybercriminals can successfully carry out fraud, identity theft, or further cyberattacks by exploiting simple human mistakes.

Attackers typically execute this method as follows:

1. Create malicious links or infected attachments disguised as legitimate files or websites.
2. Send messages via email, SMS, or social media, impersonating trusted entities.
3. Use urgency or fear to pressure the recipient into immediate action.
4. Victim clicks the link or opens the attachment.
5. Malware is silently installed, or the victim is redirected to a fake login page.
6. Sensitive data (credentials, financial information) is captured and exploited.

Why This Threat is Dangerous

Malicious links and attachments remain highly effective because they exploit human behavior rather than technical vulnerabilities.

Successful attacks may result in:

- Unauthorized access to systems and accounts
- Installation of malware or ransomware
- Compromise of sensitive or classified information
- Financial loss and identity theft
- Spread of infection across networks or units

Warning Signs to Watch For

Personnel must remain vigilant for the following indicators:

- Unexpected messages from unknown or unverified senders
- Messages that create urgency (e.g., “Act now,” “Immediate response required”)
- Suspicious or misspelled email addresses and domains
- Links that appear shortened, altered, or inconsistent with official websites
- Unexpected attachments, even from known contacts
- Requests for passwords, OTPs, or sensitive personal information

Recommendations

In this regard, AFP personnel are advised to follow these protective measures:

- Avoid clicking on suspicious or shortened links
- Do not open unexpected attachments, even if they come from known or trusted contacts
- Verify the sender’s identity before clicking any links or opening attachments

- Keep antivirus software and systems updated to detect and block threats
- Report suspicious emails or messages immediately to cybersecurity personnel
- Use only official and secure communication channels for sensitive information

If you believe you have downloaded or opened a suspicious file:

- Immediately disconnect the device from the internet or network to limit potential spread or data exfiltration
- Stop all interaction with the suspicious link, attachment, or message
- Do not enter or save sensitive information after exposure
- Change passwords immediately for any affected accounts using a secure, uncompromised data
- Run a full antivirus or anti-malware scan
- Report the incident to your cybersecurity or ICT office
- Follow incident reporting procedures and chain of command

Conclusion

Malicious links and attachments remain one of the simplest yet most effective methods used by cyber adversaries. These attacks rely on deception, urgency, and human error to succeed.

Think before you click. Verify before you act. Maintaining vigilance and following proper cybersecurity procedures are essential to protecting AFP personnel, systems, and operations.

Source: https://www.kaspersky.com/resource-center/threats/malicious-html-attachments?