Malware

Spotting the Threat

The email threats faced by organizations today vary greatly in complexity, volume, and impact. Here we take a closer look so you can spot the threat before it harms you or your organization.

Cybercriminals use email to deliver documents containing malicious software, also known as malware. Typically, either the malware is hidden directly in the document itself, or an embedded script downloads it from an external website.

Common types of malware include viruses, Trojans, spyware, worms, and ransomware, a favorite of cybercriminals who use it to infect networks and lock email, data, and other critical files until a ransom is paid.

To get victims to click, attackers will disguise malware links or files with enticing names, like 'payroll file' or 'merger plans.' You can avoid malware by:

- Refraining from clicking links or downloading attachments in suspicious emails.
- Recognizing signs of phishing emails that deliver malware and avoiding or reporting them.
- Being a healthy skeptic when evaluating emails you receive.

The sample email highlights some of the clues you can watch for.

Example

Team, ◀ Generic greetings are commonly used in phishing emails.

Per the attached revised deck (F1Q.3) please note the change in lines D1-D7 which have been updated to reflect the impact of COVID-19 losses and projected quarterly deficits.

▲ Losses and quarterly deficits are tempting lures.

This document replaces the file sent earlier in error. Sorry for any confusion.

Downloadable file attachments should be regarded with a healthy skepticism. ◀

- JMS

▲ Generic sign-offs are commonly used in phishing emails.