AUT-9 · Mobile Threat Catalogue

Archived: 2026-04-05 17:38:42 UTC

Mobile Threat Catalogue

Phishing Websites

Contribute

Threat Category: Authentication: User or Device to Remote Service

ID: AUT-9

Threat Description: Phishing emails have been prevalent for a very long time. These emails typically link to websites geared at specific individuals, departments, or companies, and may be designed to look like their genuine counterpart with the intention of capturing credentials.

Threat Origin

Phishing Defenses for Webmail Providers [1]

Exploit Examples

Your Account PayPal Has Been Limited Phishing Scam [2]

CVE Examples

Possible Countermeasures

Enterprise

Ensure corporate e-mail policy is configured to scan for suspicious files, executables, or attachments, and segregate such emails to increase end-user awareness of their potential to contain malicious content.

Deploy email and web proxy services that will examine URL resources for malicious content, and if any is found, prevent delivery of the message to the intended recipient.

Deploy email filtering tools or services that will automatically remove detected URLs from the body of emails from untrusted domains.

Educate end users on how to recognize phishing attempts and increase their awareness of techniques to browse safely from mobile devices, such as tap-and-hold on a hyperlink to examine its associated URL.

References
