T2026_02 Risks of Online Advertisements and Pop-Up Ads (March 26th, 2026)

Online advertisements and pop-up ads are a common feature on many websites and are often used to generate revenue for site operators. However, malicious actors frequently exploit advertising networks and pop-up mechanisms to distribute malware, conduct phishing campaigns, or redirect users to malicious websites. This technique, commonly known as **malvertising**, allows attackers to compromise legitimate websites or advertising platforms so that harmful advertisements are delivered to unsuspecting users. In some cases, simply viewing a malicious advertisement can trigger a redirect to exploit kits or fraudulent pages designed to steal credentials or install malware.

In corporate or government environments, these threats can have significant impacts on endpoint security. Users who interact with malicious ads may unknowingly download malware, expose login credentials, or grant browser permissions that allow persistent tracking or further exploitation. Infected endpoints can lead to unauthorized access, data exfiltration, or lateral movement within internal networks. Additionally, pop-up advertisements that mimic security alerts or software update messages may trick users into installing fake software or revealing sensitive information.

To mitigate these risks, organizations should implement layered security controls such as web filtering, DNS filtering, and browser security policies that block known malicious advertising domains. Endpoint protection platforms and secure web gateways can help detect and block malicious scripts or downloads associated with advertisements. Organizations should also enforce browser security best practices, including disabling unnecessary plugins, restricting pop-ups where possible, and ensuring browsers are regularly updated. Equally important is user awareness—employees should be trained to avoid clicking suspicious ads, unexpected pop-ups, or prompts that request software downloads or sensitive information. By combining technical controls with user awareness, organizations can significantly reduce the risk posed by malicious advertisements and pop-ups.

References

- Cybersecurity and Infrastructure Security Agency. (2023). *Malvertising: How to Protect Your Organization.* Retrieved from https://www.cisa.gov
- Federal Bureau of Investigation. (2023). *Internet Crime Report and Public Service Announcements on Online Scams.* Retrieved from https://www.ic3.gov
- Kaspersky. (2024). *Malvertising: What It Is and How It Works.* Retrieved from https://www.kaspersky.com
- Malwarebytes. (2024). *What is Malvertising?* Retrieved from https://www.malwarebytes.com

- SANS Institute. (2023). *Understanding and Preventing Malvertising Attacks.* Retrieved from https://www.sans.org