Training And Education: Necessary For Lowering Cyber Exposure

Kaspersky's detection systems identified more than 380,000 malicious files each day in 2021, which is a 5.7 percent increase over 2020.

The increase mirrors the increase in individuals working remotely due to the pandemic and the rise in the number of devices used around the world.

According to Kaspersky's Security Bulletin: Statistics of the Year Report, Linux OS malware and unwanted software increased by 57 percent in 2021. In the past, 91 percent of threats occurred through WindowsPE files.

Kaspersky states that 54 percent of threats were comprised of unspecified Trojans. Although the volume of many types of threats decreased in 2021, Trojan Droppers increased 2.24 percent compared with 2020. Trojan Droppers are "particularly harmful" because they deliver more sophisticated malware to a targeted device.

The number of viruses detected increased by 27 percent, and the number of worms increased by 117.5 percent.

Kaspersky recommends that users protect themselves from malware by never downloading or installing applications from untrusted sources. Also never click on links from unknown sources or suspicious online advertisements.

Kaspersky also advises users to create strong, unique passwords; install all updates, which may contain fixes to critical security issues; and never trust messages asking to disable security systems for office or cyber security software. "Malware grew by 5.7% in 2021" www.itweb.co.za (Jan. 07, 2022).

Commentary

Employees are constantly being bombarded with malware threats, so it is essential they are **trained and consistently educated on emerging threats**.

Human error is how most malware is distributed. Selecting attachments or links from untrusted or unknown sources is a common way malware is distributed, as noted above. However, malware is also distributed through phishing whereby cybercriminals send emails that have the appearance of a trusted source like a bank

or credit card company. Training on the risks associated with malware and phishing is important for limiting risk.

Consistent and continual education is also important. Monitor this platform for the latest malware and other cybersecurity threats and inform employees of any particularly dangerous threats. Include cybersafety tips in your communications to employees to keep cybersafety at the forefront of their minds.

This article is on the Bliss McKnight Practical HR Resources website, and available to members of the AIC Endorsed General Liability Insurance Program.

For more information contact risk@blissmcknight.com.

This article is based on generally accepted risk management best practices. It is not, and should not be considered, legal advice.

MATERIALS PROVIDED, NEED FOR REVIEW BY COUNSEL AND OTHERS, APPLICABILITY AND SUITABILITY OF RECOMMENDATIONS.

Attached are risk management related recommendations we believe may be of interest to you. Provision of these materials by our organization (set forth in section one above and referred to as "us", "our", or "we") does not constitute a representation of the appropriateness, adequacy or effectiveness of the recommendations.

These materials are provided as recommendations only. They address certain important Risk Management matters. They are not suggested or intended to provide for all circumstances or all considerations. Each situation is different in some respects, and the advice of counsel and, in many cases, other professionals, is required to prepare and implement an effective and lawful risk management related program, document or agreement. It is the responsibility of the local government to determine the suitability and applicability of these and other risk management materials to its particular needs and circumstances.

Copyright © 2022 Bliss McKnight Concepts, Inc. All Rights Reserved.