

CybeReady Presents Five Cybersecurity Countermeasures in Times of War

Company Recommends Defensive Position as Russian and Ukrainian Cyberwarfare Actions Threaten Businesses Globally



CybeReady

SANTA CLARA, CA, UNITED STATES,

April 14, 2022 /EINPresswire.com/ -- CybeReady, provider of the world's fastest security training platform, today presented five must-do actions for organizations concerned about the potential fallout of cyberwarfare between Russia and Ukraine. The provided recommendations come as businesses and employees globally become unwilling participants in the ongoing conflict.

Outside of physical warfare, both Russia and Ukraine have been involved in a dedicated program of cyberwarfare. Those involved in the conflict have launched cyberattacks on each other with entities supportive of Russia involved in data-wiping malware and taking websites offline with DoS attacks to prevent their use. Additionally, there have been malicious phishing-borne ransomware attacks and a range of other threats casting a sinister shadow that threatens every organization.

Since cyber-strikes between warring entities are not always contained, they often infect devices and websites that are on the periphery of the conflict. This includes both business and personal devices of individuals working onsite or remotely. Employee social media accounts are also at risk of being hacked for the purpose of distributing false information or malware. With the conflict surging, these attacks are expected to intensify with nearly everyone at risk of suffering the consequences of a sudden attack.

According to CybeReady, during such turbulent times, one should regard all emails with extra caution and double-check the sender's address carefully. Beware of requests that ask for technical assistance such as running software or helping to take down websites. These might not only be illegal but may also be used to hack systems on the corporate network. Try to remember that during times of crisis, there is an increase in phishing attempts of all kinds as hackers take advantage of the situation. In this circumstance, employees need to stay updated from both a news and computing perspective.

To be proactive in the defense of computing environments, our security experts recommend:

1. Personal computer and phones: Install the latest operating system and security updates.
2. Implement 2FA/MFA: Use a phone number or authentication app as the second factor of authentication to all important applications, social media accounts (Facebook/Meta, LinkedIn, Twitter, etc.), and personal email accounts. Backup email and ensure it is recoverable.
3. Change Passwords: If you are reusing a password in sites that hold your personal information, it is a good time to change your passwords.
4. Support a Culture of Security: Train your employees continuously, advise friends and family to do the same, and take an active role in creating a safer internet.
5. Defend Work from Home Environments: Install the operating system and security updates. If these are available you should see a notification on your computer or phone.

Especially important to business continuity in these times of uncertainty is the need for automated cybersecurity training that adapts to employee educational needs and accelerates the learning process. A more touchless approach not only speeds training, but also supports the IT team by reducing oversight requirements to ensure an empowering educational experience for employees. CybeReady's Adaptive Training Platform is a leading solution in this area that resolves training issues quickly through automation to strengthen security defenses.

"Building a culture of security throughout an organization is especially critical in situations where the volume of malicious cyber activity is at record levels," said Mike Polatsek, the Co-founder and CSO of CybeReady. "Deploying a security awareness program that provides training value fast and builds employee readiness with no IT effort whatsoever, can make a true difference for enterprises."

Tweet This: @CybeReady Presents Five Cybersecurity Countermeasures in Times of War - <https://cybeready.com/category/news>

Resources:

- CybeReady Case Studies - <https://cybeready.com/resource-center/case-studies>
- CybeReady White Papers - <https://cybeready.com/resource-center/white-papers>
- The Ultimate Guide of Security Awareness Training - <https://cybeready.com/complete-guide-cyber-awareness>

About CybeReady

CybeReady offers the world's fastest security training platform, that evolves your organization from security awareness to cyber readiness. CybeReady's solution autonomously engages more employees, more effectively, frequently, and easily. Infused with training expertise and powered

by machine learning, CybeReady's adaptive, easy-to-digest security training content program guarantees to reduce your high-risk employee group by 80%. CybeReady's fully-managed solution has been deployed by hundreds of enterprises worldwide, including the City & County of San Francisco, SodaStream, ING, StitchFix, Teva Pharmaceuticals, Avid Technology, and others, CybeReady is fully-managed, making it the security awareness training solution with the lowest total cost of ownership (TCO) available today. Founded in 2015, CybeReady is headquartered in Tel Aviv, Israel, with offices in the Silicon Valley. For more information, please visit www.cybeready.com.

Joe Austin

APR

+ 18183326166

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/568565578>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2022 IPD Group, Inc. All Right Reserved.