Cyber Talk

MUST-KNOW TIPS FOR SECURING

EMPLOYEE EMAILS IN THE AGE OF CORONAVIRUS

94% of cyber attacks start with an email.[1]

[1] Sandblast Network Solutions Brief, https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf

Google reports blocking more than 18 million coronavirus related phishing threats per day.[2]

As employees shifted from professionally managed networks to home wi-fi systems, hackers capitalized on security weaknesses. Between February and March of this year, the number of phishing attacks escalated by 667%. By April, the US Secret Service sent a warning to corporate America to stay on high alert for predatory email-based attacks.

The coronavirus has ushered in waves of anxiety, fear and distraction for many remote employee, leading them to unexpectedly fall victim to scams. Initially, the click rate on coronavirus-related scam materials hovered around 5%. Now it's 40%.[3,4]

Strings of attacks have led to password theft and the theft of sensitive corporate information.

The Better Business Bureau (BBB) reports the top three coronavirus related scams:

Phony cures and fake masks: Cyber criminals are sending emails and messages claiming that, for a fee, they can provide consumers with masks and other protective products that the government is supposedly hiding from the public.

Economic Impact Payment (Stimulus Check) Scams: These scams often attempt to lure consumers into paying fees in order to receive their checks sooner than the date that the IRS promised.

Business focused phishing scams: These scams take numerous different forms. They include false claims from supposed IT departments of a given company, offering IT support, or claiming that an employee's computer has a virus. Scare tactics can lure employees into divulging personal or organizational information.[5]

[2] Joe Tidy, Google blocking 18m coronavirus scam emails every day, BBC.com, April 17, 2020, https://www.bbc.com/news/technology-52319093
[3] Phil Muncaster, #Covid19 drives phishing emails up 667% in under a month, March 26, 2020, Infosecuritymagazine.com. https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/
[4] Wayne Rash, Coronavirus worries allow new scams to take hold, Forbes.com, April 21, 2020. https://www.forbes.com/sites/waynerash/2020/04/21/coronavirus-worries-allow-new-scams-to-take-hold/#5384c697515c
[5] Better Business Bureau, BBB tip: Top 6 coronavirus scams reported by BBB, April 3, 2020. https://www.bbb.org/article/news-releases/21989-top-6-coronavirus-scams-bbb

> Threat extraction can clean email attachments and web downloads in 1.5 seconds, while slashing administration overhead by as much as 70%.

Does your organization rely on the most advanced techniques and technologies to guard against email-based threats?

If not, here's a brief overview of must-know tips for improving your email security.

- Deploy platforms that have threat extraction capabilities, and that can vet all aspects of an email's message prior to its arrival in your users' inbox. Platforms with rules-based engines, including Natural Language Processing (NLP), threat emulation, AI-based phishing protection, AI-based fraud protection, URL reputation, emulating clicks on links and click-time protection (also called URL rewriting) are best.
- Invest in a platform that delivers clean and reconstructed versions of potentially malicious files received by email or that were downloaded from the web. These types of platforms allow for uninterrupted business flow while threat emulation takes place in the background.
- Ensure that your threat detection's AI heuristics are continually optimized against the latest threats found in the wild.
- Do your forensic and actionable intelligence networks integrate with your security information and event management (SIEM) and security operations center (SOC) infrastructure? Effective integrations enable you to accelerate investigations, and to potentially reduce any time-to-remediation.
- You'll want to be able to visualize attack vectors, see event timelines, and generally obtain as much information as possible about potential attacks.
- Can your threat intelligence analyze the code and behavior of incoming malware threats? Upgrade your architecture to get insights into who might be targeting your users, what tactics they might use next, and defense best practices.

To explore out-of-the-box, single-click set-ups that include all of these features and more, visit Check Point's Sandblast webpage.

AND EMAIL SECURITY ISN'T JUST AN IT THING...

Build a security-aware organizational culture. Remind employees of the following to help them stay secure:

- **Organizations such as the World Health Organization (WHO) will never request a password, or personally identifying information in order for users to access their resources. Nor will they send you email attachments that weren't specifically requested.[6]**
- **Beware of emails that use a 'voice of authority,' that appear to come from a legitimate source -such as a local hospital- but that were unsolicited.[7]**
- **URLs should be checked prior to clicking on them. Coronavirus related domains are 50% more likely to be malicious than others.[8]**

---

[6] Herb Weisbaum, How to avoid falling victim to a coronavirus phishing email attack, NBC News, March 6th, 2020. https://www.nbcnews.com/better/lifestyle/how-avoid-falling-victim-coronavirus-phishing-email-attack-ncna1137941

[7] Wayne Rash, Coronavirus worries allow new scams to take hold, Forbes.com, April 21, 2020. https://www.forbes.com/sites/waynerash/2020/04/21/coronavirus-worries-allow-new-scams-to-take-hold/#5384c697515c

[8] Update: Coronavirus-themed domains 50% more likely to be malicious than other domains, https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com