Published on *The National Law Review* https://natlawreview.com

# UK and US Issue Joint Cybersecurity Alert Concerning Explosion of COVID-19 Phishing Attacks

Article By:

Joseph J. Lazzarotti

In the US, many organizations anxiously awaiting assistance under the CARES Act are becoming the targets of cyberattackers looking to feed off of the massive relief being provided by the US treasury. Yesterday, the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) issued a joint alert warning of a substantial increase in these attacks, providing helpful guidance concerning the nature of the attacks and related information.

Specifically, the alert provides information on exploitation by cybercriminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice. The alert notes that the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations.

Organizations may not be able to prevent all attacks, but there are steps they could take to minimize the chance and impact of a successful attack, and to be prepared to respond. Here are just a few of those steps.

## Before an Attack

1. **Build the right team**

- Ensure you have an IT team in place, whether internal or through a third-party vendor, that is well-versed in emerging threats and prepared to support the organization in the event of an attack.

2. **Secure the systems**

- Conduct a risk assessment and penetration test to understand the potential for exposure to malware.

- Implement technical measures and policies that can prevent an attack, such as endpoint security, multi-factor authentication, regular updates to virus and malware definitions/protections, intrusion prevention software and web browser protection, and monitor user activity for unauthorized and high risk activities.

3. **Make your employees aware of the risks and steps they must take in case of an attack**

- This is particularly critical now – educate employees on how to recognize phishing attacks and dangerous sites — say it, show them, and do it regularly. This includes instructing them to use caution when clicking directly on links in emails, even if the sender appears to be known — verify web addresses independently.

- Employees should avoid revealing personal or financial information about themselves, other employees, customers, and the company in email, including wiring instructions. If they must, they should confirm by phone.

- Direct employees to pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (*e.g.,* .com vs. .net).

- Instruct employees on what to do immediately if they believe an attack has occurred (*e.g.,* notify IT, disconnect from network, and other measures) and what *not* to do (*e.g.,* deleting system files, attempting to restore the system to an earlier date, and the like).

4. **Maintain backups**

- Backup data early and often.

- Keep backup files disconnected from the network and in separate locations.

5. **Develop and practice an "Incident Response Plan"**

- Identify the internal team (*e.g.,* leadership, IT, general counsel, and HR).

- Identify the external team (*e.g.,* insurance carrier, outside legal counsel, forensic investigator, and public relations).

- Outline steps for organizational continuity — using backup files and new equipment, safeguarding systems, and updating employees.

- Plan to involve law enforcement (*e.g.,* FBI, IRS, Office of Civil Rights, and so on).

- Plan to identify, assess, and comply with legal and contractual obligations.

- Practice the response plan with the internal and external teams, reviewing and updating the plan to improve performance.

**After an Attack**

6. **Secure your systems**

- Review and follow your Incident Response Plan.
- Avoid compromising your investigation! This includes being careful to preserve firewalls, network and other access and activity logs and artifacts on the system that could have valuable information needed to confirm whether or not a breach occurred.
- Determine whether all malware has been removed and systems are protected from future attacks, including whether the attack is completed or ongoing, and, if ongoing, how to contain it.
- Evaluate feasibility of restoring the affected systems for normal use, mindful of the need to preserve information necessary for a forensic investigation, litigation defense, and enforcement agency inquiry.
- Monitor restored systems for a period of time.

7. **Consult legal counsel and other key vendors**

- Data breaches can trigger obligations under federal and state privacy laws, as well as contractual and ethical obligations. Obligations include notifying affected persons and federal and state agencies, as well as providing credit monitoring and identity theft resolutions services. Experienced legal counsel can help the organization navigate the maze of federal and state mandates.
- In cases of ransomware, recovering encrypted data can be complex and uncomfortable for the organization, particularly if faced with a demand for a ransom payment. Organizations should consider options carefully.
- Members of IT staff may not have sufficient experience with the latest cybersecurity tools and attack methodologies to provide competent and efficient direction. Be sure your team is experienced.
- Consulting with your insurance broker or cyber-insurance carrier is important not only to confirm applicable coverage, but because seasoned insurance professionals can provide valuable early guidance.

8. **Investigate the incident**

- Determine what happened, when, and the method the hackers used to carry out the attack.
- Identify which systems were affected and the nature of the data affected (*e.g.,* protected health information ("PHI")).
- Identify the total number of individuals (in each state of residence) whose data was affected.
- Confirm whether evidence shows that the affected data was accessed, acquired, and/or exfiltrated to the outside of your systems.
- Evaluate what mitigation measures were in place (e.g., were the affected files encrypted, extent of data backup, and so on).

9. **Provide notifications, if needed**

- Determine whether state or federal laws, or other obligations, require notification.
- Federal and state agencies and credit monitoring bureaus may need to be notified based on a number of factors, including the states of residence of the persons affected and the number of persons affected.
- Be sure notification include mandatory disclosure and are provided within applicable time frames.
- Credit monitoring, call center, and other services also may be required or appropriate under the circumstances.

10. **Lessons learned**

- Prepare an Incident Response Report including the *Who? What? Where? When? Why? How?*
- Review the Incident Response Report with all internal and external team members to learn from and prevent future attacks.

No doubt the threat of an attack has increased based on the joint report referenced above. At the same time, hardening an organization's environment has become particularly more challenging in this environment. Increasing awareness among employees to avoid becoming a victim of a phishing attack could be an excellent initial step.



National Law Review, Volume X, Number 100

Source URL:https://natlawreview.com/article/uk-and-us-issue-joint-cybersecurity-alert-concerning-explosion-covid-19-phishing