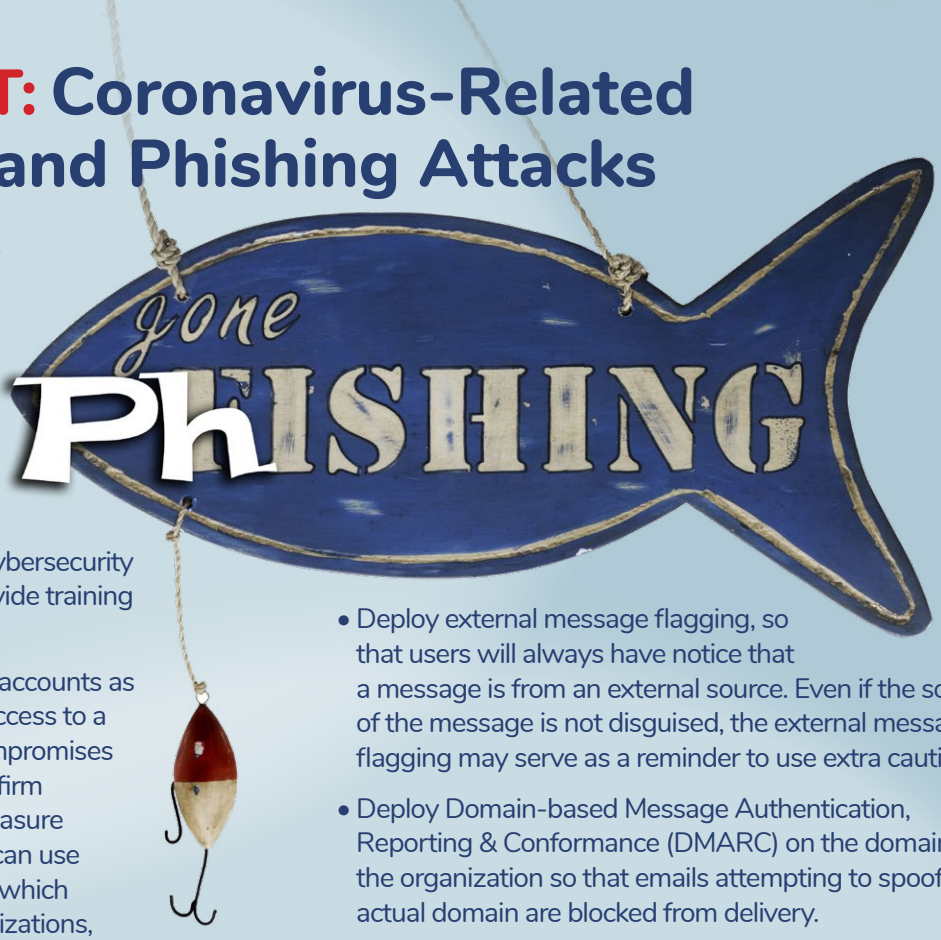
ATTPRO ALERT: Coronavirus-Related Ransomware and Phishing Attacks



The use of sophisticated Coronavirus-related phishing and malware attacks has been on the rise with new malicious email campaigns surfacing each day. Hackers are also expected to take advantage of millions of vulnerable remote connections from employee home networks to their corporate networks. Now, more than ever, it's important to establish cybersecurity procedures for your law firm, and provide training on those policies.

Malicious attackers often target email accounts as a means to gain user credentials for access to a computer network. Email account compromises pose serious risks to law firms. A law firm employee's email account can be a treasure trove of sensitive data that a criminal can use for malicious purposes. These emails, which appear to come from legitimate organizations, contain content such as advice on combatting the Coronavirus and phony alerts from the World Health Organization (WHO) or Centers for Disease Control and Prevention (CDC). The email messages contain either an attachment or a link to a malicious website – both of which appear to be legitimate. Clicking on the attachment or the link may cause malicious software (malware) to be downloaded onto the device used to open the email message. The malicious website may also direct the employee to log in to continue. The log in process, which allows the attacker to gain access to their personal information and to compromise the security of their employers' networks, will result in the theft of user credentials.

The recent emergence of these schemes demonstrates that businesses must remain vigilant. As law firms prepare for the potential implications that the Coronavirus outbreak will have upon their businesses and employees, they should include in their plans strategies for educating their employees on how to prevent phishing and malware attacks.

- Do not click on suspicious attachments or links.
- Deploy external message flagging, so that users will always have notice that a message is from an external source. Even if the source of the message is not disguised, the external message flagging may serve as a reminder to use extra caution.
- Deploy Domain-based Message Authentication, Reporting & Conformance (DMARC) on the domain of the organization so that emails attempting to spoof the actual domain are blocked from delivery.
- Deploy multi-factor authentication. In addition to requiring a user name and a password to access an email account, multi-factor authentication requires at least one additional piece of information to access the account. The concept of multi-factor authentication is to provide a secondary level of protection in order to validate online accounts beyond solely a username and password. Multi-factor authentication tools help prevent malicious actors from hijacking email accounts and using them for malicious purposes.
- Provide employees access to a virtual private network (VPN) so they can establish a secure connection to WiFi from home. Many VPNs are available online or in the app store. Prices vary, but tend to be $20 per month: a small investment to ensure your firm's cybersecurity.
- Use phishing reporting tools in Outlook and Gmail to block online attacks and alert the IT admin at your firm.

Don't let your law firm's network become infected. Utilize these tips to educate employees and establish effective cybersecurity safeguards!

Christopher E. Ballod, CIPP/US, CIPP/E is a partner in the Philadelphia and Pittsburgh offices of Lewis Brisbois, a vice chair of the Data Privacy & Cybersecurity Practice, and a member of the Corporate, and Complex Business & Commercial Litigation Practices.

Sean Hoar is a partner in the Portland office of Lewis Brisbois and chair of the Data Privacy & Cybersecurity Practice.