Cyber Risks & Liabilities

Research Shows Malicious Document Downloads Are Surging

Using malicious software—also called malware—to compromise a victim's data or technology is one of the most common cyberattack methods. Malware is typically triggered by clicking on the deceptive links or dangerous attachments that often accompany phishing emails. In fact, recent research found that malicious document downloads are currently on the rise.

According to Netskope Threat Lab's latest report, 40% of malware attacks have been deployed through the medium of harmful email attachments during 2021, representing a 20% rise over last year's data. Specifically, these email attachments have been disguised as office documents—including Microsoft Office files, PDFs and Google Docs.

This rise in malicious document downloads is likely tied to cybercriminals taking advantage of shifting work arrangements during the ongoing COVID-19 pandemic. After all, the significant increase in remote operations over the past year has led to more employees relying on digital platforms (e.g., email and online messaging) to communicate with their co-workers.

With remote employees using virtual mediums to share important information and files, cybercriminals have been able to trick some of these workers into downloading malicious office documents via deceitful emails. For instance, a cybercriminal may impersonate a victim's co-worker and email them a harmful file titled "Monthly Financial Report" in order to manipulate them into downloading it.

In light of this trend, it's critical for employers to take the following steps to protect against malicious document downloads:

- Educate employees on how to recognize and respond to phishing emails. In particular, workers should always verify the sender's identity by double-checking their address before interacting with an email and avoid opening any attachments from unknown sources. Further, employees should report any suspicious email activity to the IT department.
- Implement antivirus programs and endpoint detection and response systems on workplace technology to help minimize malware threats. Update this software regularly.
- Install email security features (e.g., spam filters) to help prevent malicious messages from landing in employees' inboxes altogether.

For more risk management guidance, contact us today.

Educate Employees on This Emerging Phishing Scam

While phishing scams have been a persistent issue for employers of varying sizes and sectors, cybersecurity experts recently confirmed that a new phishing tactic has emerged.

This scam entails cybercriminals impersonating a trusted cybersecurity company and emailing their victims a "secure message." The email then asks victims to click on a harmful link to view their "secure message." However, clicking on the link opens a malicious website that attempts to compromise victims' devices.

So far, this emerging phishing tactic has been detected in over 75,000 employees' email inboxes across industry lines. The

message is typically sent to multiple employees within the same organization, often from different departments. Targeted employees have included both individual contributors and those in leadership positions.

It's vital for employers like you to educate workers on the latest phishing tactic. Be sure to show employees the key signs of this scam and encourage them to report suspicious messages to the IT department.

Cybersecurity Considerations for Hybrid Work

The COVID-19 pandemic has greatly changed how employees across the country work and live. That is, the past year saw a substantial proportion of the workforce transition to remote operations. Looking ahead, a recent study found that the majority of remote employees (83%) are wanting to continue working from home in some capacity. As a result, nearly half (45%) of employers are planning to implement hybrid work arrangements in the near future. Such arrangements allow for employees to split their time between working remotely and on-site. For example, employees may work in the office every Monday and stay remote for the remainder of the week.

While hybrid work models can offer various benefits to both employers and their workforces, these arrangements also carry unique cybersecurity risks. First, remote work environments often provide less secure network settings than on-site setups, leaving employees more vulnerable to cloud-based cyberattacks. In fact, such attacks have skyrocketed by over 600% since the pandemic began.

What's worse, by alternating between remote and on-site networks, employees could potentially expose a greater proportion of workplace technology and assets amid a cyber incident. In other words, if an employee unknowingly has their laptop hacked by cybercriminals while working remotely and connects that device to an on-site network a few days later while working in the office, all workplace technology is then at risk of being compromised by the hackers. If you are considering a hybrid work model within your organization, consider these best practices to help minimize cybersecurity exposures:

- **Utilize a virtual private network (VPN).** Having a VPN provides your employees with a private, protected network connection—both remotely and on-site. VPNs offer various cybersecurity features, such as hiding users' IP addresses, encrypting data transfers and masking users' locations. If you don't already have a VPN, this is a crucial step in developing a secure hybrid work model, as it can reduce network vulnerabilities when employees work remotely. If you already have a VPN, be sure it is fully patched.
- **Train employees.** Require staff to participate in routine cybersecurity training. This training should help employees stay up to date on the latest cyberthreats, emerging attack methods and top tips for protecting against these concerns. Additionally, this training should address specific risks related to hybrid work arrangements and how to properly mitigate them.
- **Safeguard all devices.** Make sure all workplace devices—including those used remotely—are equipped with adequate security software (e.g., antivirus programs, firewalls, endpoint detection and response systems, and patch management products). Ensure this software is updated as needed to maintain its effectiveness.
- Foster open communication. Lastly, encourage employees to consult the IT department if they encounter any cybersecurity issues or suspect a potential cyberattack.

Contact us today for additional cybersecurity resources.

BeaconPath