opentext™

Phishing in a Pandemic: 1 in 4 Americans Received a COVID-19 Related Phishing Email

9/22/2020

Global survey finds overall email volume has increased 34% since last year, without a corresponding increase in cyber security protection

WATERLOO, ON, Sept. 22, 2020 /PRNewswire/ -- **OpenText™** (NASDAQ: OTEX), (TSX: OTEX) released a new report, **COVID-19 Clicks: How Phishing Capitalized on a Global Crisis** that sheds light on what people know about phishing attacks, what makes them click on a potentially malicious link and overall cybersecurity and cyber resilience habits in the time of COVID-19.

"With mass work from home, an influx of emails and a general 'always connected' attitude, there are more opportunities for cybercriminals than ever before," said OpenText CEO & CTO Mark J. Barrenechea. "We saw phishing URLs impersonating streaming services skyrocket during quarantine, as cybercriminals target people where they are most often. Businesses and consumers must prioritize cyber resilience and recognize that it is everyone's responsibility to protect their data."

The report suggests companies and consumers alike are falsely confident when it comes to cybersecurity. Nearly all respondents worldwide (95%) recognize that phishing remains a problem for companies and consumers, yet more than three quarters (76%) admit to opening emails from unknown senders, with over half (59%) blaming it on the fact that phishing emails look more realistic than ever before. The survey also revealed an opportunity for more security awareness education. Just 59% believe they know what to do to keep their data safe, with nearly one third (29%) admitting they've clicked on a phishing scam in the last year and one in five (19%) confirming receipt of a phishing scam related to COVID-19.

In the report, Dr. Prashanth Rajivan, assistant professor at the University of Washington, offered his perspective on how the COVID-19 pandemic and general increase in working from home could affect individuals' and businesses' cybersecurity status. "Like with distracted driving, working while doing other household chores or even watching TV seems easy enough when doing mundane tasks, such as email processing. But this type of distraction can also make people vulnerable. People might be less likely to properly notice and weigh the risks of a potential phishing message."

Read the full report **COVID-19 Clicks: How Phishing Capitalized on a Global Crisis**

Key Global Findings:

Phishing risks remain high, with more opportunities as the number of emails increase, workers log into corporate networks remotely and hacks look more real than ever before:

- On average, survey respondents receive approximately 70 emails per day, a 34% increase over last year. More emails mean more opportunity for attack and more cognitive load to discern what's legitimate and what's a fraudulent request.
- One in five respondents received a phishing email related to COVID-19.
- 45% of people are shopping online more often, although 68% believe that there is a greater risk their credit and financial information could be exposed.
- 42% have accessed their backed-up data to recover a file since COVID-19 began, as more people connect from home on new or additional devices and need to retrieve their files.

Companies and consumers are falsely confident when it comes to cyber safety. Despite knowing the risks, they're still taking chances with their data, and that's impacting their cyber resilience:

- Only 59% of employees believe they know enough to keep themselves and their personal data safe from cybersecurity attacks.
- But 64% of employees said they would open an email from their boss first, followed by 23% who would open an email marked as "URGENT" first, underlining people's vulnerability to **business email compromise** attacks.
- 22% of respondents admit to clicking a phishing link in their personal email while approximately 14% clicked one in their work email, suggesting employees may let their guard down outside of work.
- Just 14% said employees are responsible for cyber resilience within their company, with 74% ascribing responsibility to IT or senior leadership.

More education and prevention measures are critical to achieve cyber resilience, especially remote workers who need to access company resources from personal or shared public networks.

- Even though the pandemic has brought a new reliance on cloud and collaboration services like Microsoft® 365, only 54% of respondents said they or their company **backup their Microsoft 365 files**, leaving a huge gap in data recovery plans.
- Only 21% of respondents claim their company has increased cybersecurity training during the pandemic,

despite an influx of attacks and more risk associated with a distributed workforce.

- Just 60% think their company is cyber resilient, demonstrating a general lack of confidence in what companies are doing to help protect consumers and employees from hackers.
- 81% of people take steps to determine if an email is malicious, but one third still admit they've clicked on a scam in the last year.
    - 64% look at the sender address
    - 64% check if the email contains suspicious attachments
    - 56% look for misspellings or bad punctuation in the email
    - 45% check the link address (by hovering over link)
    - 29% do an internet search for the sender's name/company
- 14% of respondents admit they do nothing to determine if a message is malicious – these employees need to be identified and given additional cybersecurity training and coaching.

Additional Resources

- **COVID-19 Clicks: How Phishing Capitalized on a Global Crisis**
- **COVID-19 Clicks Report Infographic**
- **Webroot Security Awareness Training**
- **Carbonite Backup for Microsoft 365**
- **Carbonite Endpoint**

Report Methodology:

Webroot, an OpenText company, partnered with Lewis Research to survey 7,000 office professionals from the U.S., U.K., Japan, Germany, France, Italy, Australia and New Zealand in June 2020.

About OpenText

OpenText, The Information Company™, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit **opentext.com**.

OTEX-G

View original content to download multimedia:**http://www.prnewswire.com/news-releases/phishing-in-a-pandemic-1-in-4-americans-received-a-covid-19-related-phishing-email-301134037.html**

SOURCE Open Text Corporation