COVID-19 CLICKS: How Phishing Capitalized on a Global Crisis

The COVID-19 pandemic has undoubtedly changed how we think about work and the professional landscape. With more people working from home than ever before, there has also been an explosion in remote work-related phishing URLs. As of July 2020, there have been 365% more phishing URLs related to COVID-19 in the US compared to March 2020. How did that happen? And more importantly, how can we prevent phishing in our future?

For Businesses:

1. Educate employees. Phishing is a social engineering attack. Empower your employees to fight phishing by sharing phishing prevention tips and resources. Ensure your employees understand that phishing attacks often use their personal information and induce them to share it. Evaluate phishing training and adjust your training course to meet your employees’ requirements.

2. Implement employee behavior monitoring. Employees may not always recognize phishing attempts. Implementing employee behavior monitoring can help you ensure effective phishing protection. Use a platform that can quickly flag employees who may be engaged in phishing attempts.

3. Keep up to date with phishing attacks. Phishing attacks are becoming more prevalent. Studies show that 25% of employees respond to phishing attempts. It’s important to know how prevalent phishing attacks are and to understand the current state of security.

4. Use two-factor authentication. Two-factor authentication is a security mechanism that requires two forms of authentication from the user: something they know (e.g. a password), and something they have (e.g. a smartphone). If both authentication factors are verified, the user can access the account.

5. Use anti-phishing software. Anti-phishing software can help detect and prevent phishing attacks. Such software analyzes URLs and email addresses to determine if they are legitimate or not.

6. Keep your systems updated. Phishing attackers often exploit security holes in older software versions and operating systems. It’s important to keep your operating systems and software updated to prevent such attacks.

7. Install antivirus software. Antivirus software can help protect your computer from malware. It’s important to ensure your antivirus software is up to date and that it scans your system regularly.

8. Maintain a healthy dose of suspicion. Phishing attackers often try to induce you to click on a link or download an attachment. By being vigilant and maintaining a healthy dose of suspicion, you can significantly reduce the amount of uncertainty that comes with online threats.

For Individuals:

9. Keep your systems updated. Phishing attackers often exploit security holes in older software versions and operating systems. It’s important to keep your operating systems and software updated to prevent such attacks.

10. Use two-factor authentication. Two-factor authentication is a security mechanism that requires two forms of authentication from the user: something they know (e.g. a password), and something they have (e.g. a smartphone). If both authentication factors are verified, the user can access the account.

11. Install antivirus software. Antivirus software can help protect your computer from malware. It’s important to ensure your antivirus software is up to date and that it scans your system regularly.

12. Maintain a healthy dose of suspicion. Phishing attackers often try to induce you to click on a link or download an attachment. By being vigilant and maintaining a healthy dose of suspicion, you can significantly reduce the amount of uncertainty that comes with online threats.

Learn More
Read the full report and get even more tips for staying safe.
webroot.com/click