COVID-19 CLICKS

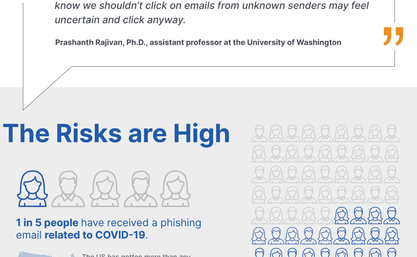
How Phishing Capitalized on a Global Crisis

The COVID-19 pandemic has undoubtedly changed how we do things. In particular, more people have begun working from home than ever before. With the massive increase in remote work, there has also been an explosion in cybercriminal activity like phishing. Not only is phishing still prevalent, but it continues to be on the rise.

We surveyed 7,000 office workers in the US, UK, Australia/New Zealand, Germany, France, Italy and Japan on their understanding of phishing, their email and click habits, and how their online lives have changed since the beginning of the COVID-19 pandemic. Here's an overview of the findings from around the globe.

Less than 3 out of 5 of workers worldwide think they know enough to keep themselves and their data safe from cyberattacks.

8 in 10 say they take steps to determine if an email message could be malicious.



Percentage of people who admit to having fallen victim to a phishing scam on either their personal or work email accounts in the last year.

3 in 10 workers worldwide are certain they've clicked a phishing link in the past year. **In the US, it's 1 in 3.**

> *People aren't great at handling uncertainty. Even those of us who know we shouldn't click on emails from unknown senders may feel uncertain and click anyway.*
>
> **Prashanth Rajivan, Ph.D., assistant professor at the University of Washington**

The Risks are High

1 in 5 people have received a phishing email **related to COVID-19**.

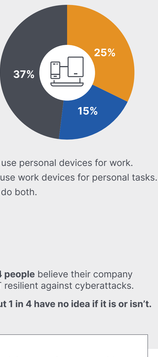
The US has gotten more than any other country (1 in 4), suggesting phishers may be targeting the Americans more heavily.

We've seen a massive spike in phishing URLs that target COVID-related topics. For example, with people spending more time at home, use of streaming services has increased.

In March 2020 alone, phishing URLs targeting popular streaming services jumped by...

- YouTube 3,064%
- HBO 525%
- Twitch 337%

And during the overall lockdown period from March to July 2020, phishing URLs targeting Netflix jumped 646%.[1]



54% of people have increased the amount of time they spend working from home.

> *People are taking increased physical safety measures in the pandemic, including mask wearing, [etc.] This heightened level of precaution and awareness could cause people to slightly overestimate their overall safety, including their safety regarding online threats*
>
> **Prashanth Rajivan, Ph.D., assistant professor at the University of Washington**

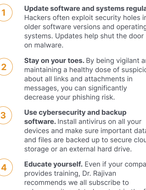
We All Need to Do Better

54% of people click emails from unknown senders regularly.

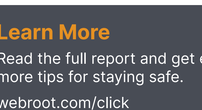
74% don't back up their data to ensure its recoverable in the event of a cyberattack.

***Yet 42%** have needed to recover lost files since the pandemic began.*

Only 21% of workers say their companies have increased cybersecurity training during the pandemic.



25% use personal devices for work.
15% use work devices for personal tasks.
37% do both.



1 in 4 people believe their company ISN'T resilient against cyberattacks.

About 1 in 4 have no idea if it is or isn't.

> *If we want to enable employees to assess risk properly, we need to cut down on uncertainty and blurring of context lines. That means both educating employees and ensuring we take steps to minimize the ways in which work and personal life get intertwined."*
>
> **Prashanth Rajivan, Ph.D., assistant professor at the University of Washington**

How to Stay Cyber Resilient Now and In the Future

FOR BUSINESSES

1. **Know your risk factors and over prepare.** Once you've assessed the risks, you can create a stronger data breach response plan.
2. **Ensure workers have clear distinctions between work and personal time, devices, and obligations.** This helps reduce the amount of uncertainty that can ultimately lead to phishing-related breaches.
3. **Back up data and make sure employees can access and retrieve data no matter where they are.** Accidents happen; what matters most is being able to recover quickly and effectively. Don't forget to back up collaboration tools too, such as Microsoft® Teams and the Microsoft® 365 suite.
4. **Invest in your people.** Empower your people with regular training to help them successfully avoid scams and exercise appropriate caution online.

FOR INDIVIDUALS

1. **Update software and systems regularly.** Hackers often exploit security holes in older software versions and operating systems. Updates help shut the door on malware.
2. **Stay on your toes.** By being vigilant and maintaining a healthy dose of suspicion about all links and attachments in messages, you can significantly decrease your phishing risk.
3. **Use cybersecurity and backup software.** Install antivirus on all your devices and make sure important data and files are backed up to secure cloud storage or an external hard drive.
4. **Educate yourself.** Even if your company provides training, Dr. Rajivan recommends we all subscribe to cybersecurity-related content in the form of podcasts, social media, blogs, and reputable information sources to help keep strong, cyber resilient behavior top-of-mind.

Learn More

Read the full report and get even more tips for staying safe.

webroot.com/click

CARBONITE an opentext company | WEBROOT an opentext company

[1] These numbers represent real-world threat intelligence from the Webroot® Platform.