20
Feb

hing

The 2023 Gone Phishing Tournament Results: Everything You Need to Know

The results of Fortra's Gone Phishing Tournament are here, and they highlight the potential power and danger of phishing across the world.

This global test uncovered that 1 in 10 individuals are susceptible to these attacks, which would have led to 90,000 compromised passwords if the campaign had been an actual cyber attack.

This year's tournament featured an updated email and landing page to reflect evolutions in phishing attacks, leading to a whopping 60% of users compromising their work password after they clicked on the initial phishing link.

These results show that despite being one of the cyber threats with the most awareness and training surrounding it, the evolution of phishing is so rapid that even well-trained users remain potential liabilities when faced with this attack.

This article will give an overview of the Gone Phishing Tournament, provide critical stats from the report, and explain what to expect around phishing in the coming year.

What is Gone Phishing Tournament?

The Gone Fishing Tournament is a yearly event that allows companies worldwide to evaluate and optimize their phishing training by gaining precise and reliable benchmarking data based on their employee performance, industry data, and regional specifications.

This year, over 300 organizations participated, amounting to over 1.37 million end-user participants, making it one of the largest phishing tests of its kind worldwide.

Fortra once again collaborated with industry leader Microsoft to devise a convincing phishing landing page and expired password notification.

This scenario allowed the monitoring of several potentially problematic behaviors by users, such as clicking on a phishing link and entering their password on a fraudulent landing page, while filtering by geographical location and industry.

Summary of Findings from the Gone Phishing Tournament

- 4% click-through rate on phishing simulation emails, marking a 3.4 percentage point increase from the previous year. (Note: the 2022 simulation template used a different context but targeted the same behaviors with its tactics).
- 5% of recipients submitted their passwords in the form embedded in the malicious webpage, a 3.5 percentage point rise from 2022, with 60% of clickers eventually compromising their passwords.
- For click rates by industry, the Finance sector posted the lowest click rate (6.2%) across all industries for the second year. The Transport sector (6.8%) came in second, followed by the Manufacturing sector at 7.7%. Conversely, the Education sector saw both the highest click and password submission rates, totaling 16.8% and 12.2%, respectively.
- Geographical trends showed South/Latin America with the best performance (7.8% click rate, 3.9% password submission) and the Asia and Pacific region the worst (14.9% click rate, 9.2% password submission). Europe scored a click rate of 9% and a password submission rate of 5.6%, while North America finished with totals of 10% and 6.5%, respectively.
- Organizations with less than 100 employees posted the highest click rate (12.9%) despite being the size segment with the lowest click rate in 2022. Organizations with an employee count between 100 and 499 had the highest overall password submission rate (7.3%).

The Secret to Launching Effective Phishing Simulation Training

With the attention called to phishing attacks in recent years, users have received a lot of training on this threat, and companies in all industries have begun notifying clientele about the risks of phishing. This situation has led to an overreliance on technical safeguards provided by software and a false sense of security derived from the training received.

Phishing is an ever-evolving threat that can change every month. While regular training is important, it must be paired with phishing simulations to provide your users with adequate context

Search

Search...

Categories

- Compliance and Governance (9)
- Cyber Security Awareness (298)
- Data Privacy Awareness (57)
- Events (11)
- GDPR (9)
- News (25)
- Phishing (91)

Recent Posts

- What is Baiting in Cyber Security?
- 7 Smishing Examples and How to Protect Yourself
- What is Swatting? What to Look for and How to Defend Yourself
- The 2023 Gone Phishing Tournament Results: Everything You Need to Know
- Protect your loved ones from phishing, social engineering and other cyber attacks

Tags

byod CISO Communication tools Covid-19 Scams credential stuffing attacks Cyber Security Awareness cyber security professional Data breaches Data Privacy End user engagement gartner magic quadrant GDPR Training governance Human Risk information security awareness information security program lise lapointe malware National Cyber Security Awareness Month NCSAM Password phishing Phishing scams phishing simulation ransomware Remote working Security Awareness Framework Security Awareness Training social engineering Social Networks Work from home and identify any potential weaknesses to the new variations.

Phishing simulations are a core component of a cyber security-aware work culture. Free events like the Gone Phishing Tournament are an excellent way to truly grasp the power of data in cyber security training and recognize the importance of investing in a complete solution.

It's important to know that phishing simulations must be used as a tool not only to identify problem users but also to improve your future training. The data gathered during a phishing simulation is especially useful as it gives you a snapshot of your company's skill level and understanding of cyber security trends.

From reducing click rates to maximizing training course completion rates, it all starts with the right data.

Maximizing results with risk-based phishing training campaigns

With increases across the board in observed statistics this year, it's fair to say that the fight against phishing is one that companies will have to keep engaging in for years to come. The low cost and high scaling potential of phishing as a cyber threat will always make it an enticing cyber attack for criminals worldwide.

While mandated phishing training is now common, the results of the Gone Phishing Tournament demonstrate the need for alternative and immersive solutions such as gamified tests and phishing simulations. Simply relying on traditional training can leave your staff unprepared to handle the rapidly evolving threat of phishing with your company data on the line.

Solutions like phishing simulations have a proven effect on phishing click rates and provide organizations with crucial data to alter their training programs.

Reserve a free copy of the report here to take the first step in building a cyber security culture in your workplace.

RESERVE MY REPORT

Share: f 𝕏 in t

Newer
← What is Swatting? What to Look for and How to Defend Yourself

Older
Protect your loved ones from phishing, social engineering and other cyber attacks →

TRAINING

Cyber Security Training for Employees
Privacy Awareness
Click and Launch
Compliance and Governance
GDPR
Phishing Simulation
Cyber Games

GET STARTED

Free Demo
Request a Quote
Phishing Simulation Trial

FREE TOOLS

Cyber Security Hub
eBook – The Human Fix to Human Risk
Phishing Free Trial
Reports and Guides
Cyber Challenges Demo

STAY CONNECTED

f in 🐦 ▶

COMPANY

About Terranova Security
Join Our Team

GET IN TOUCH

Contact Us
Customer Support
Cybersafe and Sound Newsletter

SUBSCRIBE TO THE CYBERSAFE AND SOUND NEWSLETTER

Your cyber security awareness newsletter

SIGNING UP FOR NEWSLETTERS INDICATES YOU AGREE WITH OUR PRIVACY POLICY.

IF YOU DECIDE THAT YOU NO LONGER WANT TO RECEIVE OUR NEWSLETTERS, YOU CAN UNSUBSCRIBE BY CLICKING THE "UNSUBSCRIBE" LINK, LOCATED AT THE BOTTOM OF EACH NEWSLETTER.

Privacy Policy | Cookie Policy

FORTRA
Terranova Security®