The Human Factor

Cybersecurity, Ransomware and Email Fraud in a Year that Changed the World

proofpoint.

As the global pandemic upended work and home routines, cyber attackers pounced. And now in 2021 we are seeing what happens when emboldened cyber criminals press their advantage.

People-focused attacks require a people-centric defence, one that recognises the three fundamental facets of cybersecurity risk…

Vulnerability

How likely are your users to become a victim of a cyber attack?

20% of users failed **attachment-based** cyber threat testing
Those that include a malicious file.

12% of users failed **link-based** cyber threat testing
Those that include an unsafe URL that leads to malware and harmful websites.

4% of users failed **data entry-based** cyber threat testing
Those that take the user to a fake login page to steal credentials and other personal data.

Some of the most successful attack techniques in 2020 were also the most targeted, used in campaigns that sometimes comprised only a handful of emails.

Steganography: hiding malicious code in pictures and other file types. More than **1 in 3 people** targeted clicked on malicious steganography email

CAPTCHA: Using visual puzzles to tell human from machine. Click rates **increased 50X** year on year

Attacks

What threats do your users face?

The pandemic was the most popular lure in 2020. Almost every threat actor used COVID-themed content at some point.

Whatever the lure, attack methods varied…

- Credential phishing accounted for almost **two-thirds** of malicious messages
- **25% of attack campaigns** hid malware in compressed executable files
- **10% of campaign-related malicious email** attempted to distribute Emotet malware
- Remote access Trojans appeared in nearly **25% of all email** threat campaigns
- **More than 48M messages** contained malware capable of being used as an entry point for ransomware attacks.

10x Excel 4.0 macro attacks

Fivefold Password-protected file attacks

18% Thread hijacking attacks

2019 vs 2020

Privilege

How much damage would an attack cause?

The more privileged a compromised account, the more access to sensitive and valuable data. And the more damaging a cyber attack.

Hybrid and remote working has increased the risk of insider threats – whether malicious or negligent.

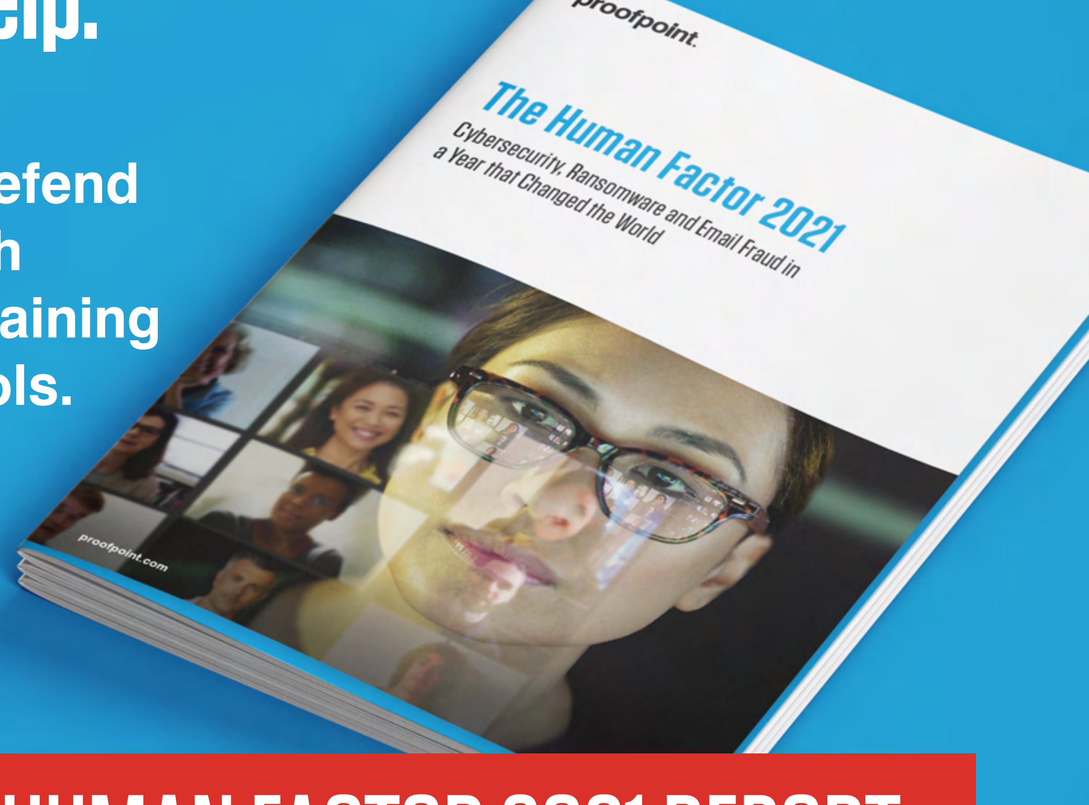
Top management insider threat management alerts:

- Connecting an unlisted USB device copy
- Exfiltrating tracked file to the web by uploading
- Opening a clear text file that potentially stores passwords
- Downloading File with Potentially Malicious Extension
- Performing large file or folder copy during irregular hours
- Exfiltrating a file to an unlisted USB device
- Installing hacking or spoofing tools
- Accessing upload and sharing cloud services

Solving the people problem

Cyber attacks are inevitable. But most can't succeed without human help.

Arm your people to defend your organisation with security awareness training and risk-based controls. Find out more...



DOWNLOAD THE HUMAN FACTOR 2021 REPORT

For more information, visit proofpoint.com

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com.**

proofpoint.