ThriveDX

THE TOP 5 PHISHING ATTACKS IN 2022 AND WHAT TO DO ABOUT THEM

It-sa, Oct-26th-2022

Palo Stacho

Palo Stacho

Security Awareness Expert and Strategic consultant ThriveDX

Study Director Global Awareness Study 2020 & 2022

Co-Founder LUCY Security

Free Agent at securityawareness.guru

Since 2015 dozens of awareness projects D / A / CH and UAE among others also for banks, Lufthansa Group, Bosch, FRoSTA, Swisscom or Mobiliar Insurance

Hacked? LUCY Awareness Training powered by ThriveDX provides remedy...

THE security awareness solution to immunize employees!

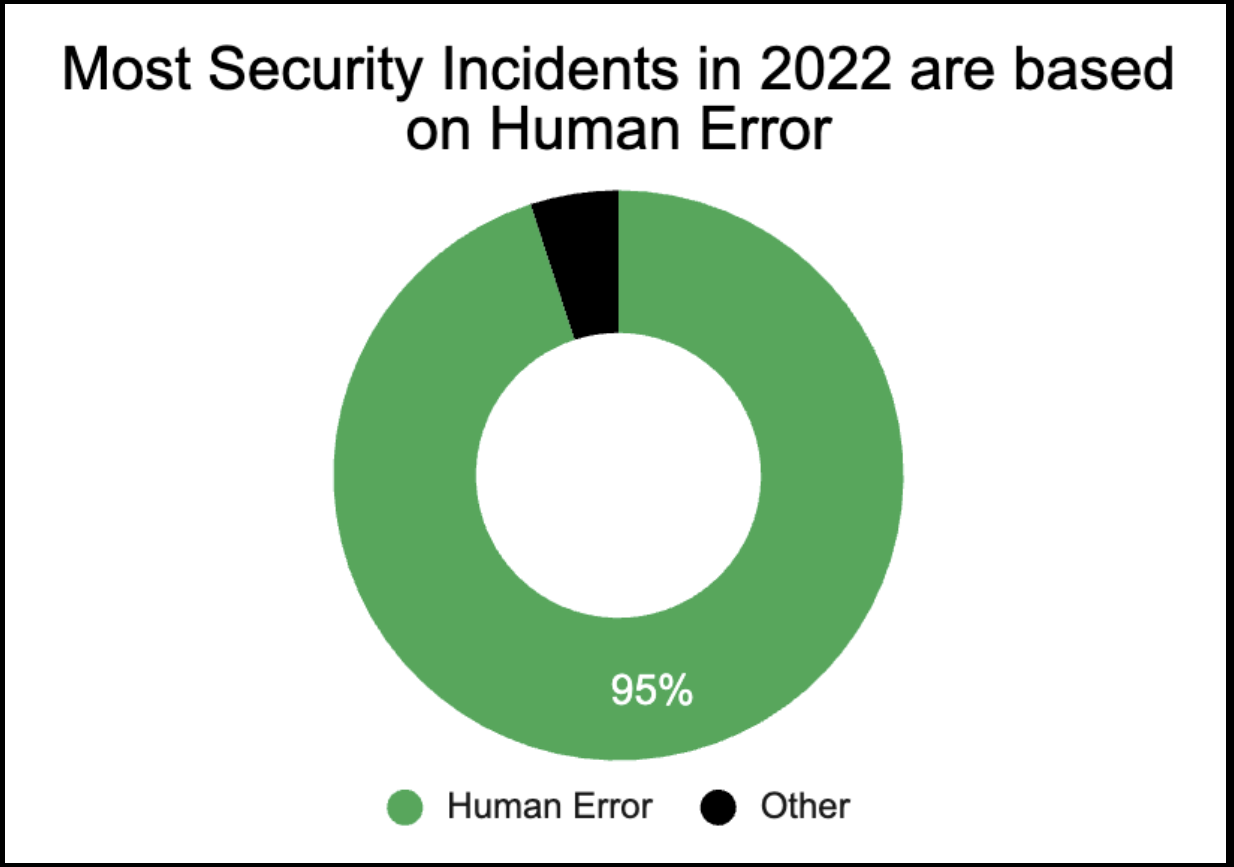
Phishing Simulator, LMS, PhishButton, Analysis, 350 Courses, 150 Videos

Agenda

1. **Top 5 Phishing Attacks**
2. Phishing Attack Trends
3. What to do against it?
4. Great Phishing Simulations, effective Trainings, Success Factors

Did you know that...

95% of cyber incidents are attributed to human error
(IBM Cybersecurity Report)



Firewall, Antivirus & Co are not enough anymore!

Identity Theft Resource Center (USA) - First Quarter 2022 Data Breach Analysis

Phishing / Smishing / BEC remains most significant Attack Vector

Attack Vector	2022 YTD
Cyberattacks	**367**
Phishing/smishing/BEC	110
Ransomware	67
Malware	22
Non-secured Cloud Environment	3
Credential Stuffing	2
Unpatched software flaw	-
Zero Day Attack	-
Other	9
NA – not specified	154

ITRC IDENTITY THEFT RESOURCE CENTER

Call Now 888.400.5530

idtheftcenter.org

First Quarter 2022 Data Breach Analysis:
Data Compromises Off to Fast Start; Victim Rates Continue to Drop

Summary

- Publicly reported data compromises totaled 404 through March 31, 2022, a 14 percent increase compared to Q1 2021.
- This is the third consecutive year when the number of total data compromises increased compared to Q1 of the previous year. It also represents the highest number of Q1 data compromises since 2020.
- The number of individual victims, though, dropped in Q1 2022. The 20.7M victims in this reporting period is a −50 percent decrease compared to Q1 2021 and a 41 percent drop from Q4 2021.
- Approximately 92 percent of the data breaches in the first three months of 2022 were the result of cyberattacks.
- Phishing and Ransomware remain the #1 and #2 root causes of data compromises; however, a majority of data breach notices in Q1 2022 did not list a root cause of the breach.
- System & Human Errors represent ~8 percent of the Q1 2022 data compromises.
- Data breaches resulting from physical attacks such as document or device theft and skimming devices dropped to single digits (3) in Q1 2022.

Discussion

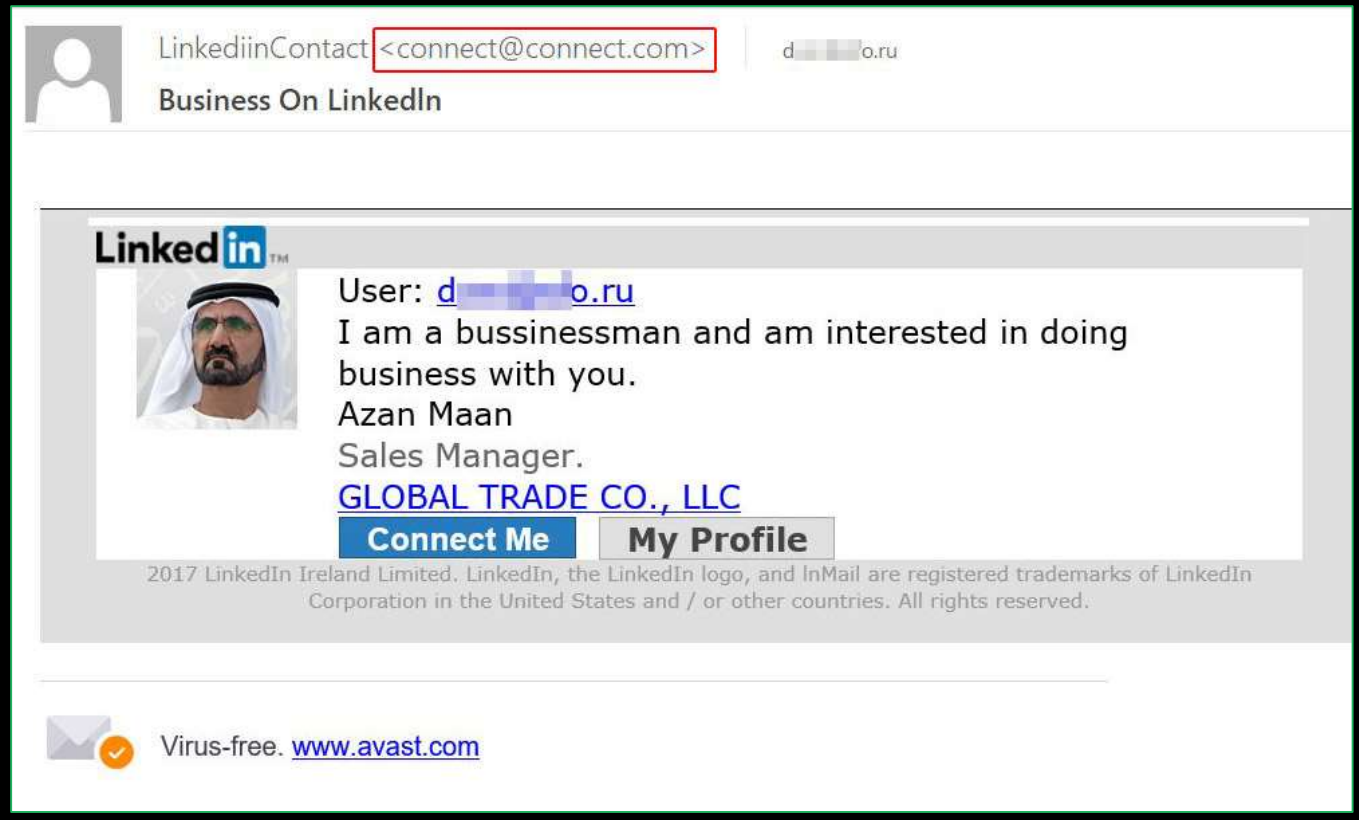
- After a record-breaking year for data compromises in 2021 (1,862), Q1 of 2022 begins with the highest number of data compromises in the past three years. Traditionally, Q1 is the lowest number of data breaches reported each year.
- Cyberattacks that lead to data compromises continue to increase, representing ~92 percent of all data compromises. Phishing and related attack vectors, ransomware, and malware remain the top three root causes of cyberattack-related data breaches.
- However, continuing a trend that emerged in 2021, 154 out of 367 data breach notices did not include the cause of the breach. That makes "unknown" the single largest attack vector in Q1. That also represents a 40 percent increase of the total number of unknown breach causes for full-year 2021.
- While subsequent breach notice updates may include more attack information, the increasing lack of transparency in breach notices represents a risk to organizations as well as individual consumers.
- The only non-cyberattack-related attack vector in double digits during Q1 was related to email or letter correspondence with 12 instances.
- Healthcare, Financial Services, Manufacturing & Utilities, and Professional Services sectors had the most compromises in Q1 2022.

888.400.5530 • 2514 Jamacha Rd., Ste. 502-525 El Cajon, CA 92019-4492

ThriveDX

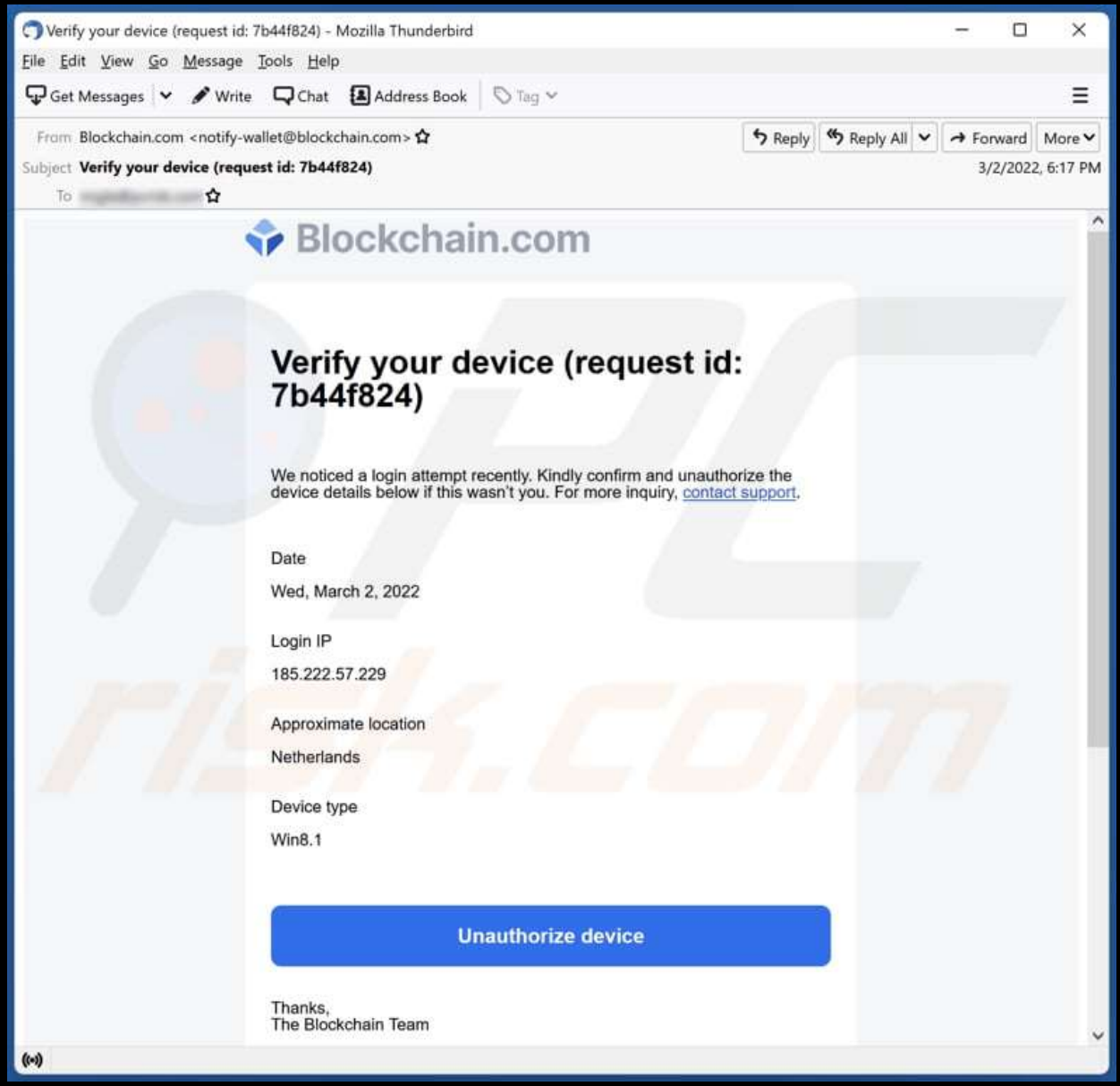
#1 - LinkedIn Phishing

52% of all phishing attacks globally in Q1 2022



#2 - Blockchain Phishing

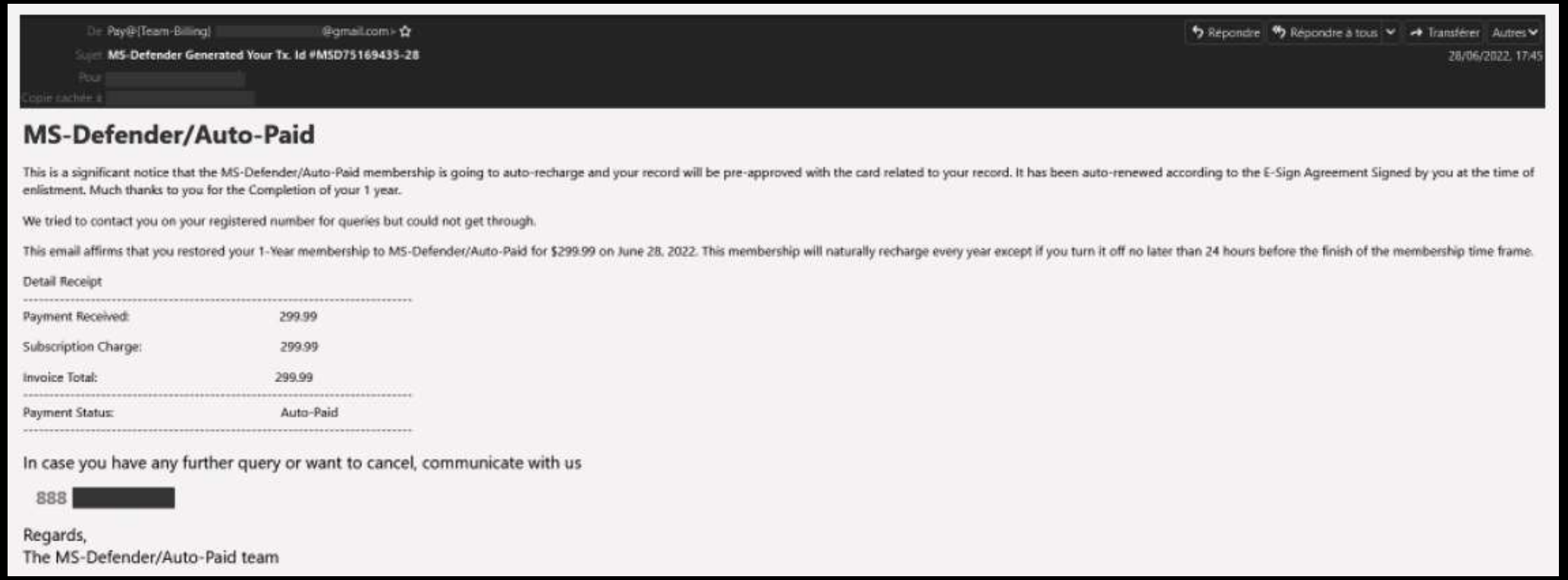
Blockchain.com, Luno, and Cardano are the top-most phished crypto projects



#3 - Microsoft Defender Support Scam

June 2022 299$ subscription payment has been billed → VISHING

Previously impersonating brands like Norton, McAffee, and Microsoft, and later, Apple and Amazon



De: Pay@[Team-Billing] @gmail.com>
Répondre | Répondre à tous | Transférer | Autres
Sujet: MS-Defender Generated Your Tx. Id #MSD75169435-28
28/06/2022, 17:45
Pour:
Copie cachée à:

MS-Defender/Auto-Paid

This is a significant notice that the MS-Defender/Auto-Paid membership is going to auto-recharge and your record will be pre-approved with the card related to your record. It has been auto-renewed according to the E-Sign Agreement Signed by you at the time of enlistment. Much thanks to you for the Completion of your 1 year.

We tried to contact you on your registered number for queries but could not get through.

This email affirms that you restored your 1-Year membership to MS-Defender/Auto-Paid for $299.99 on June 28, 2022. This membership will naturally recharge every year except if you turn it off no later than 24 hours before the finish of the membership time frame.

Detail Receipt

Payment Received:	299.99
Subscription Charge:	299.99
Invoice Total:	299.99
Payment Status:	Auto-Paid

In case you have any further query or want to cancel, communicate with us

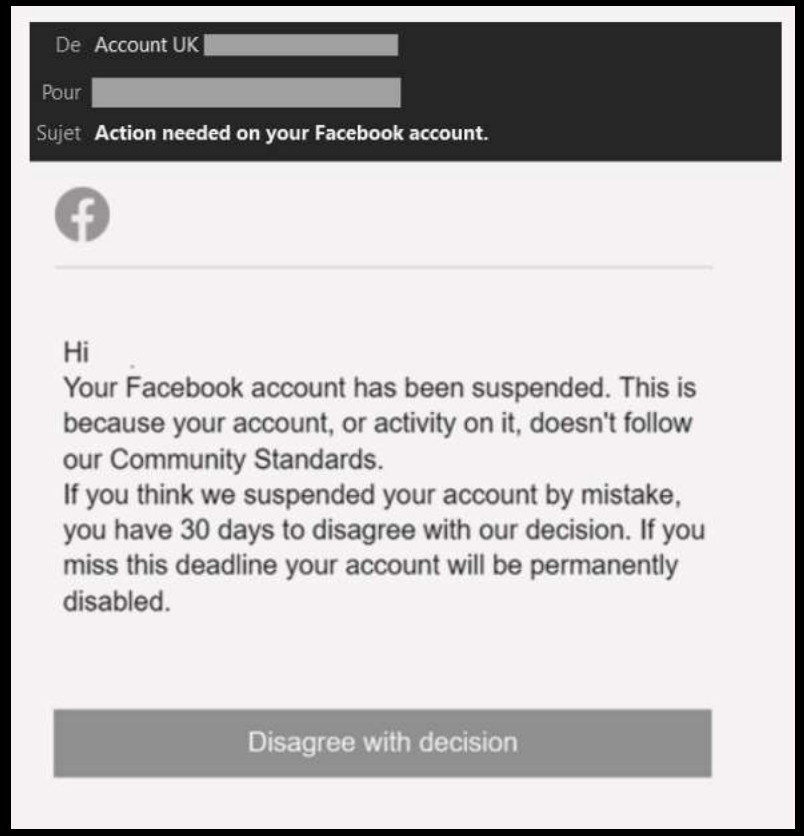
888 [redacted]

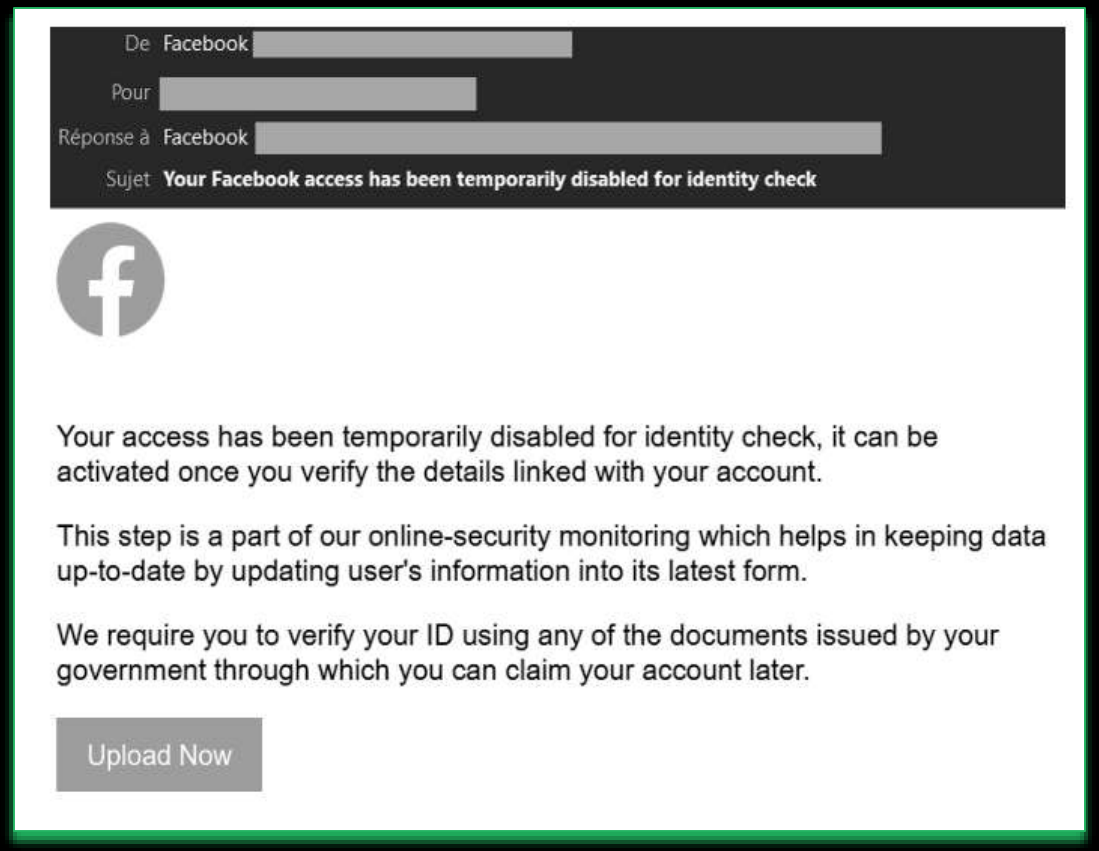
Regards,
The MS-Defender/Auto-Paid team

ThriveDX

#4 - Facebook community standards violation

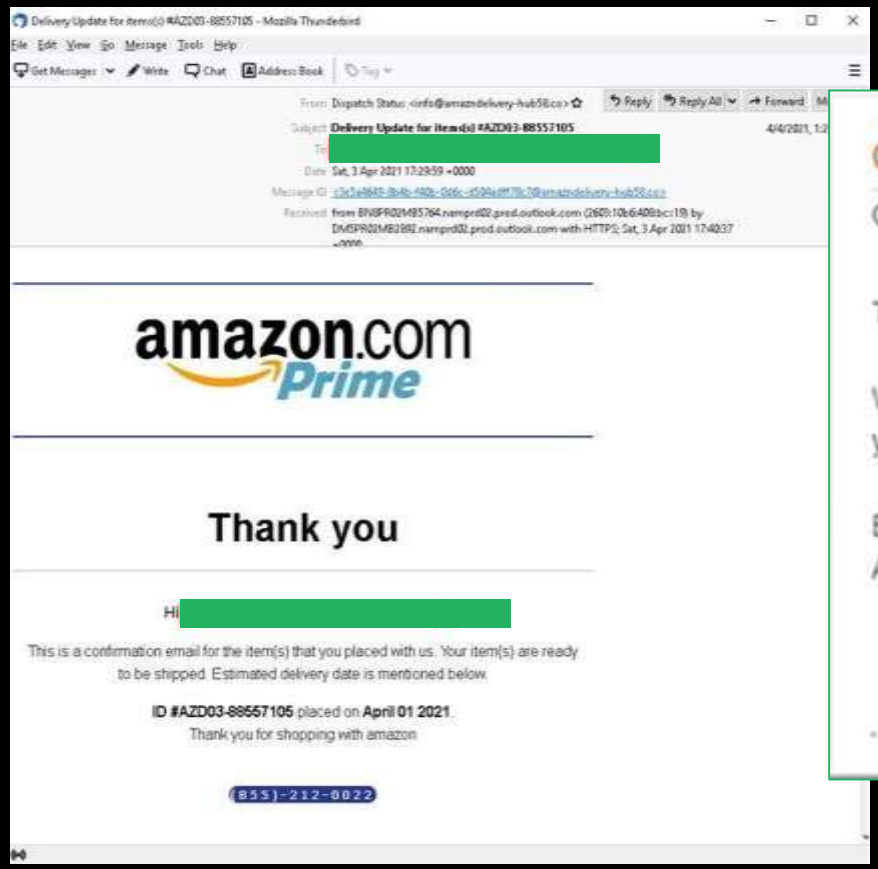
FB Account has been suspended due to a violation of “Community Standards.”

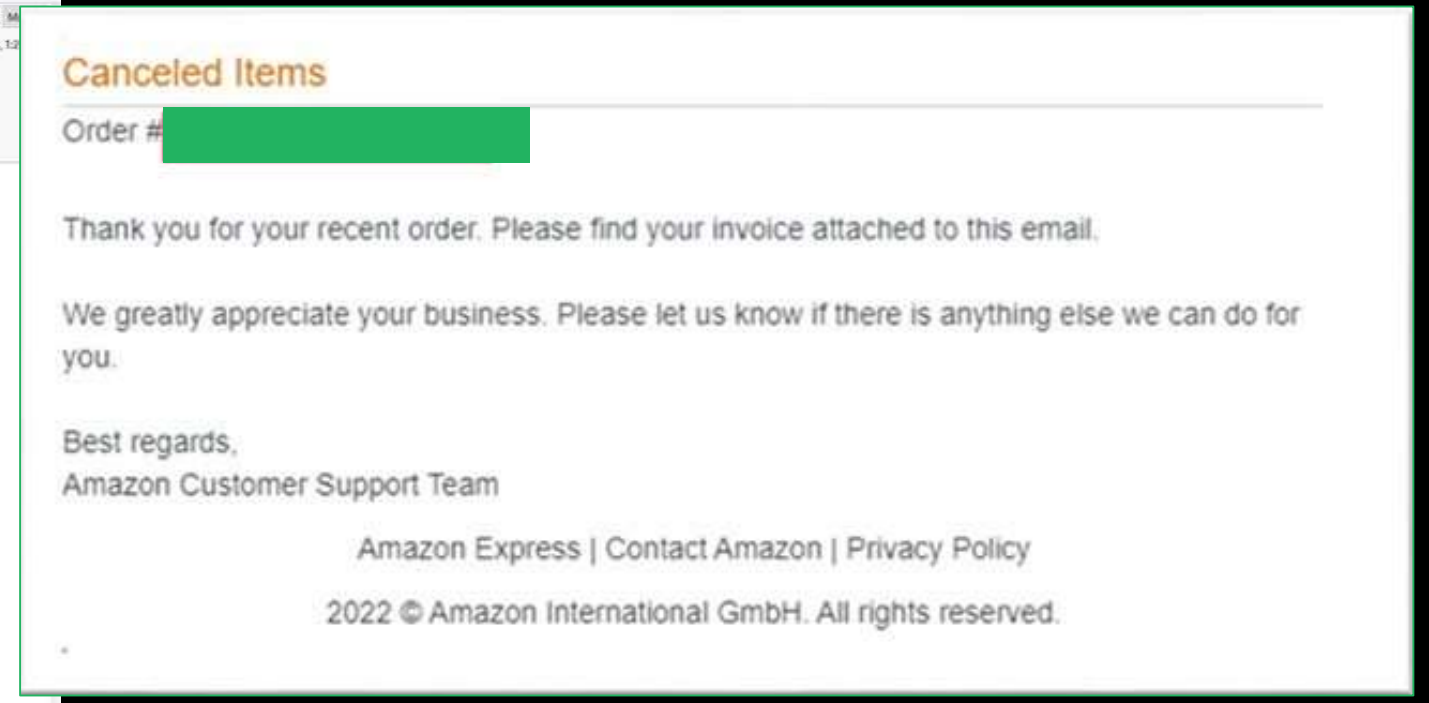




#5 – Amazon Prime Day Phishing

Most frequently impersonated - Roughly Phishing 900 Sites detected globally in 2022





#Bonus – Top Subject Lines

Lot of phishes with empty subject lines!

Research finds that 67% of cybercriminals leave the subject line blank when sending malicious emails!

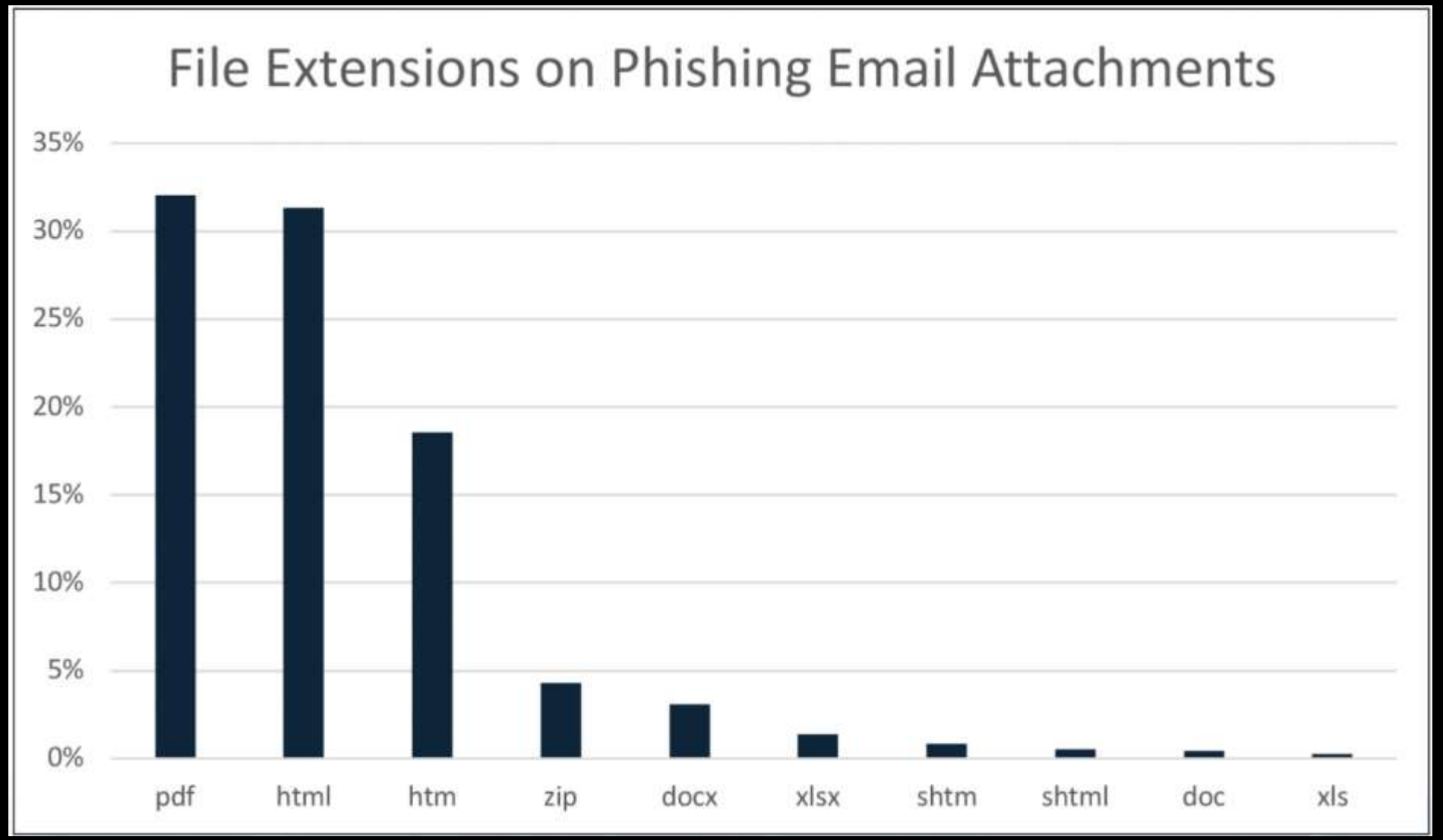
Other subject lines include

- Fax Delivery Report (9%)
- Business Proposal Request (6%)
- Request (4%)
- Meeting (4%)
- You have (1*) New Voice Message (3.5%)
- Re: Request (2%)
- Urgent request (2%)
- Order Confirmation (2%)

#Bonus – Top 11 spoofed Brands

- 1. Microsoft
- 2. Apple
- 3. Google
- 4. BMO Harris Bank (BMO)
- 5. Chase
- 6. Amazon
- 7. Dropbox
- 8. DHL
- 9. CNN
- 10. Hotmail
- 11. Facebook

#Bonus – Top 10 File Extensions 2022



Sources:

- LinkedIn Phishing https://www.kaspersky.de/blog/linkedin-phishing/27713/
- Blockchain Phishing https://www.pcrisk.de/ratgeber-zum-entfernen/11273-blockchain-com-email-scam
- Microsoft Defender Support Scam https://www.vadesecure.com/en/blog/phishers-favorites-top-25-h1-2022
- Facebook community standards violation https://www.vadesecure.com/en/blog/phishers-favorites-top-25-h1-2022
- Amazon Prime Day Phishing https://www.trendmicro.com/zh_hk/research/21/f/amazon-prime-day-big-sales--big-scams.html
- Lot of phishes with empty Subject Line https://www.globalsecuritymag.com/Top-5-phishing-statistics-of-2022,20220801,128455.html
- https://www.globalsecuritymag.com/Top-5-phishing-statistics-of-2022,20220801,128455.html
- https://www.vadesecure.com/en/blog/phishers-favorites-top-25-h1-2022
- Phishing Intelligence Trends Review Q1 2022 Cofense
- Top Domains: IBM Security X-Force Threat Intelligence Index 2022

Agenda

1. Top 5 Phishing Attacks
2. **Phishing Attack Trends**
3. What to do against it?
4. Great Phishing Simulations, effective Trainings, Success Factors

What are the Attack Trends?

3X

Click effectiveness for targeted phishing campaigns that add phone calls: The click rate for the average targeted phishing campaign was 17.8%, but targeted phishing campaigns that added phone calls (vishing or voice phishing) were three times more effective, **netting a click from 53.2% of victims.**

What are the Attack Trends?

Based on synthesis from multiple internal & external sources:

- **VISHING** and Vish+Phish on the rise
- Voice Cloning (Deep Fake) will gaining popularity
- Smishing and CFO/CEO Fraud very popular
- Fake Parcel delivery services, sextortion, and tech support scams still trending in 2022
- Brand impersonation continues to lure victims through phishing pages. Microsoft, Apple, Google and LinkedIn will remain the topmost impersonated brands
- Ukraine-themed phishing emails
- Crypto and NFTs becoming more and more a favorite
- Phishing and Ransomware remain the top root causes of data breaches in the first quarter of 2022 (ITRC)
- HTML attachments still most common files deployed by attackers.
- EMOTET, a go-to cybercrime service for malicious actors is back on stage and trending

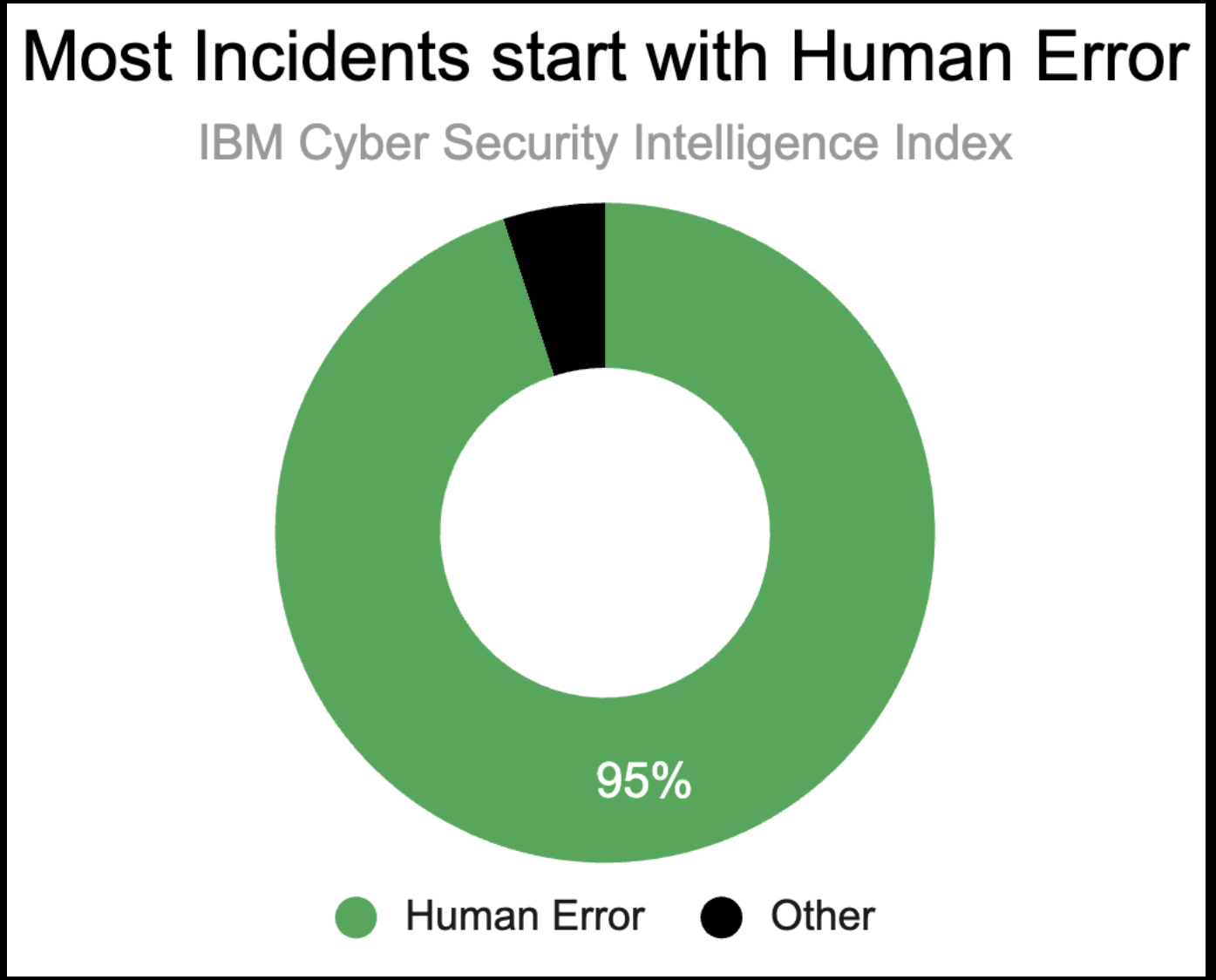
Sources:

- https://securityintelligence.com/articles/biggest-phishing-trends-2022/
- https://www.securitymagazine.com/articles/97498-4-phishing-trends-observed-in-q1-2022
- Smishing and cfo/ceo fraud very popular: https://www.all-about-security.de/threats-und-co/security-trends-2022/
- Phishing reaches all time high 2022 - https://www.helpnetsecurity.com/2022/06/15/2022-total-phishing-attacks/
- https://www.tripwire.com/state-of-security/security-data-protection/phishing-threat-trends-intelligence-report/
- https://www.securitymagazine.com/articles/97498-4-phishing-trends-observed-in-q1-2022
- Voice Cloning FBI warning April 2022 https://www.youtube.com/watch?v=sq_EWWVPTrE
- https://blog.avast.com/trending-phishing-scams-2022
- https://www.all-about-security.de/threats-und-co/security-trends-2022/
- IBM Security X-Force Threat Intelligence Index 2022 Full Report

Agenda

1. Top 5 Phishing Attacks
2. Phishing Attack Trends
3. **What to do against it?**
4. Great Phishing Simulations, effective Trainings, Success Factors

Again:
Most Security Incidents start with Human Error!



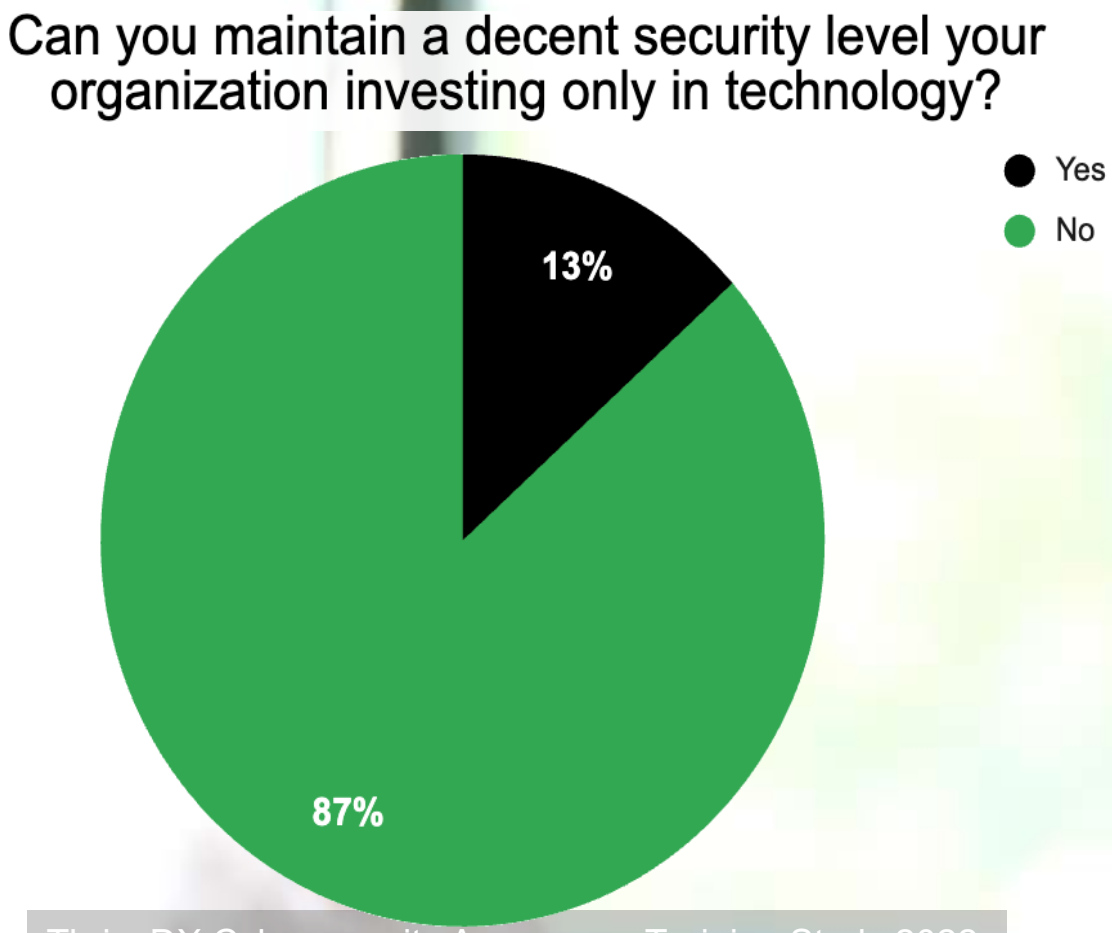
ThriveDX

So what actions can we take to counter that?

And how do you do that?

Build an Awareness Program using the right tool

Is it possible to maintain an adequate level of IT security without employees?



ThriveDX Cybersecurity Awareness Training Study 2022

The 3 Building Blocks of an effective Cybersecurity Awareness Program

Phishing Alert Button & Analysis Process

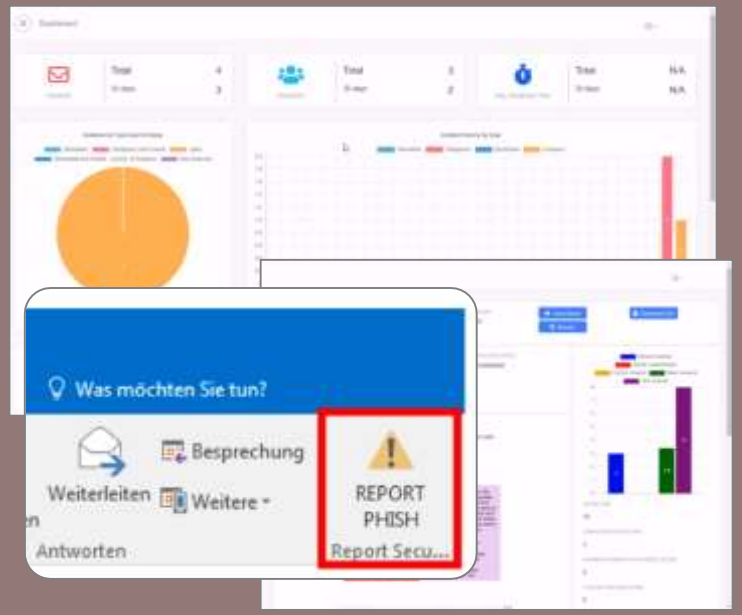
Training

[Sm]Phishing Simulations

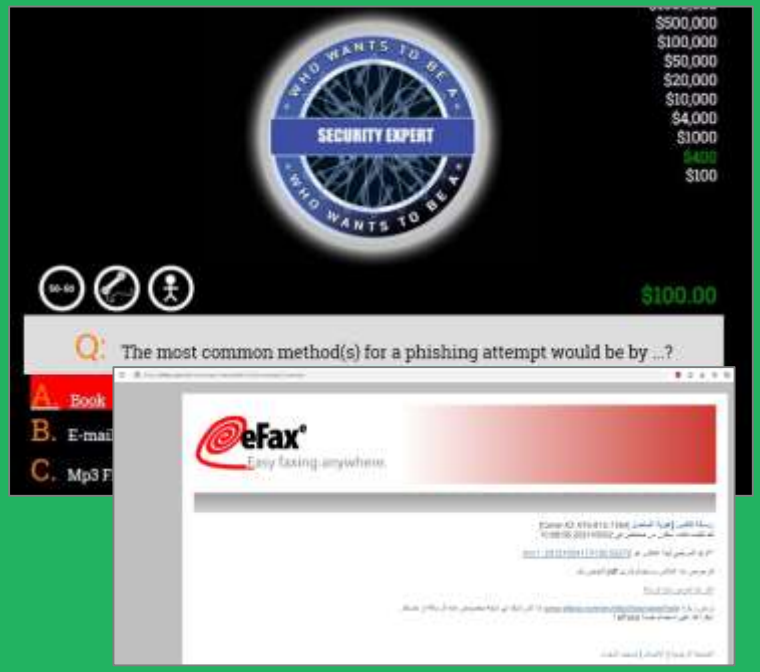
Enabler: Lucy Awareness Training powered by ThriveDX - *Cloud or On-Premise*

Implementation of an Awareness Program

Email Threat Management
„Engage, Alarm & Analyse“



Awareness Campaigns
„Test & Train“



Infrastructure Audits
„Malware-Sim / Mailfilter Test“

Reporting

Agenda

1. Top 5 Phishing Attacks
2. Phishing Attack Trends
3. What to do against it?
4. **Great Phishing Simulations, effective Trainings and Success Factors**

ThriveDX

Great Phishing Simulations

ThriveDX

Lucy
Powered by ThriveDX

2022 Global Cybersecurity Awareness Training Study

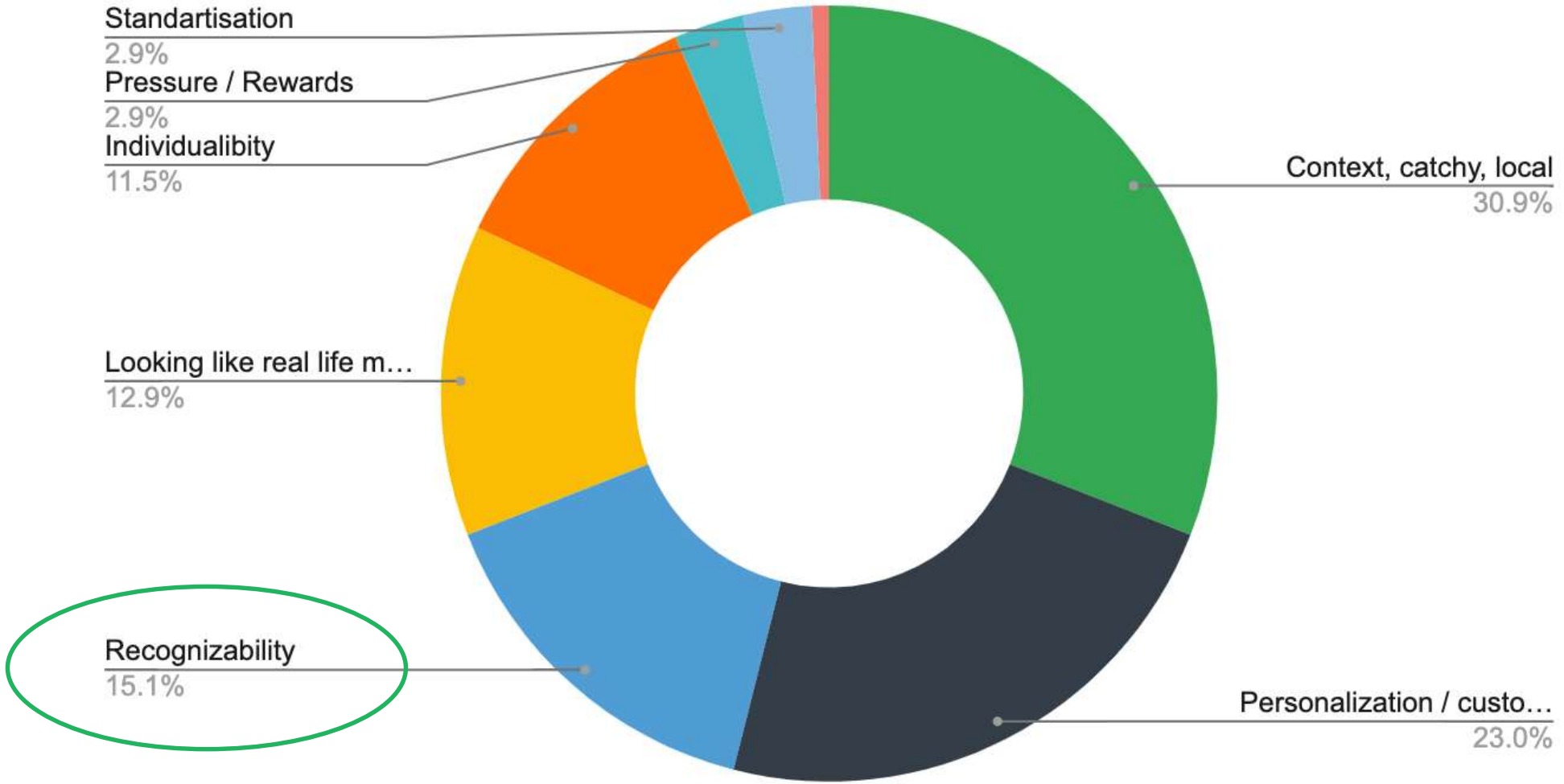
Research and
data collected
collaboration

> “What is a good phishing simulation? One where as many as possible 'fall in' or a simulation with the highest possible reporting rates.”
>
> **Study participant**

August 2022

ThriveDX

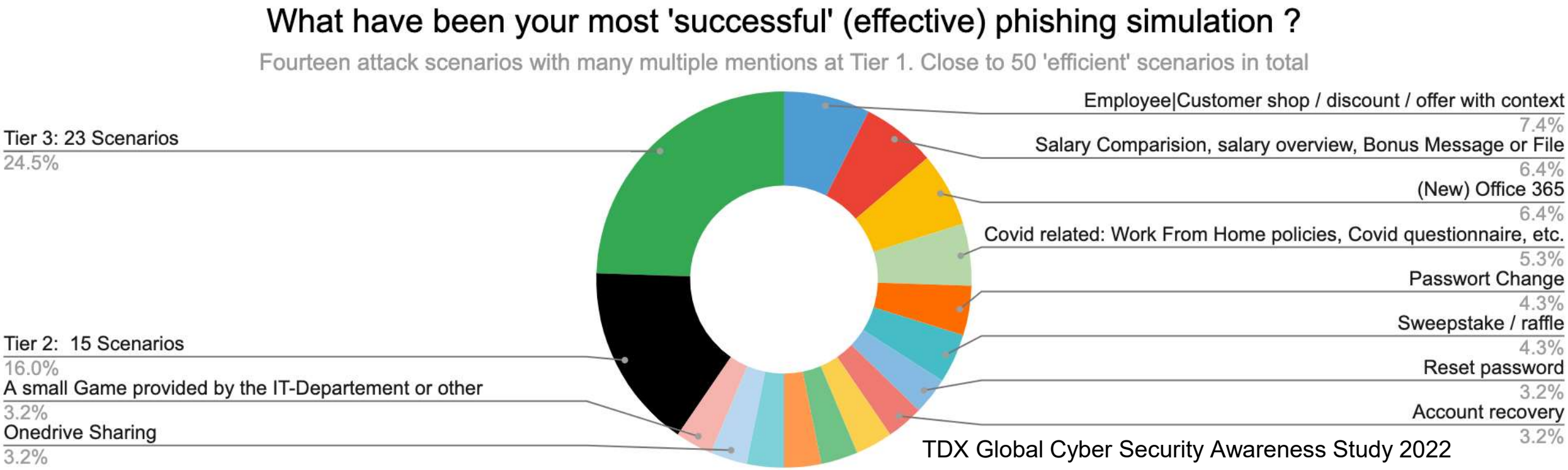
What are the success factors for **a ‘good’ Phishing Simulation?**



TDX Cyber Security Awareness Training Study 2022

ThriveDX

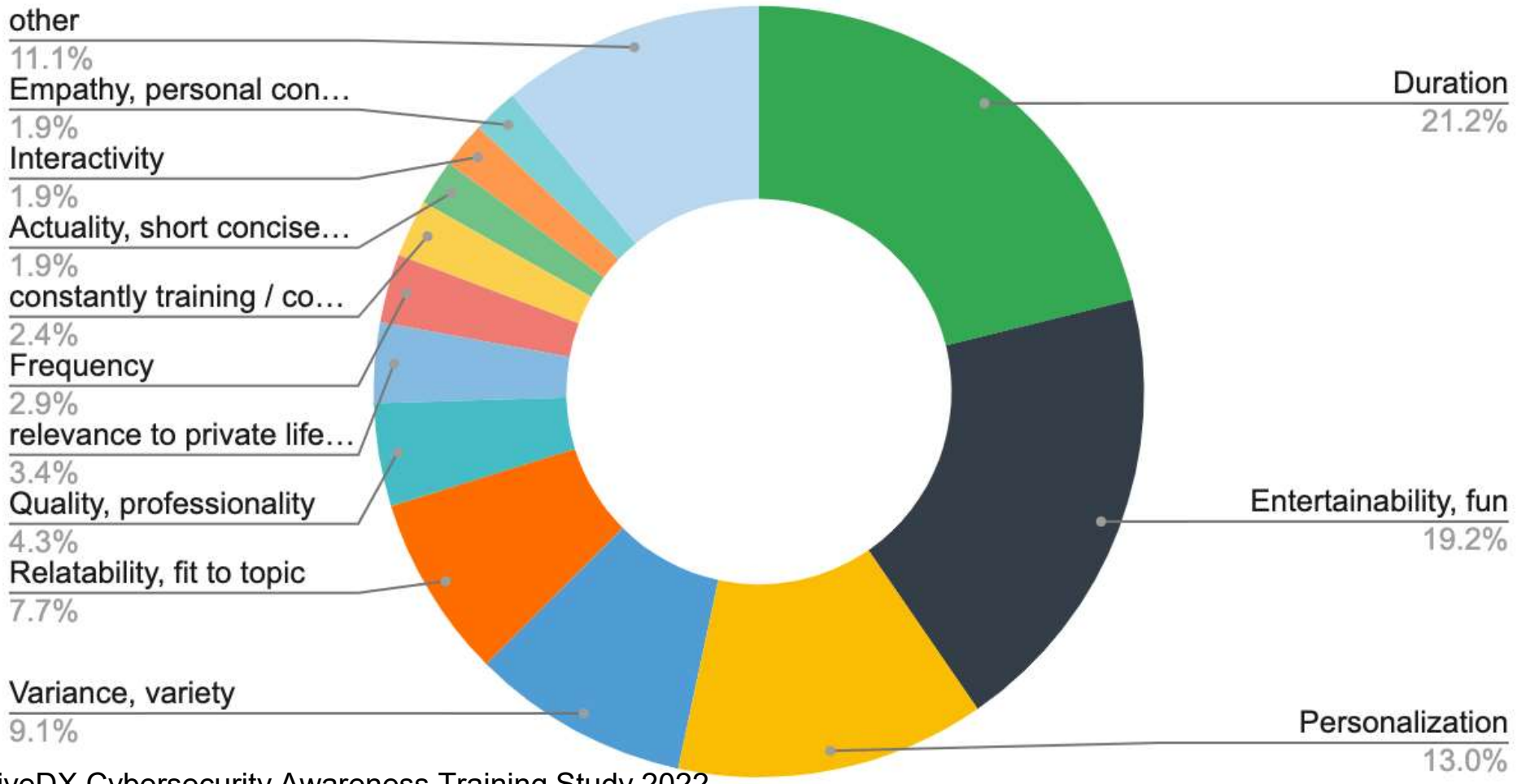
What was your most ‘successful’ Phishing Simulation?



It was often mentioned that basically 'all' phishing simulations seem to work if a plausible company context with the right language can be established in the attack scenario. The most successful scenarios are those that appeal to the emotional level: Curiosity, sense of duty, urgency, helpfulness, greed, profit, empathy and personal appeal.

ThriveDX

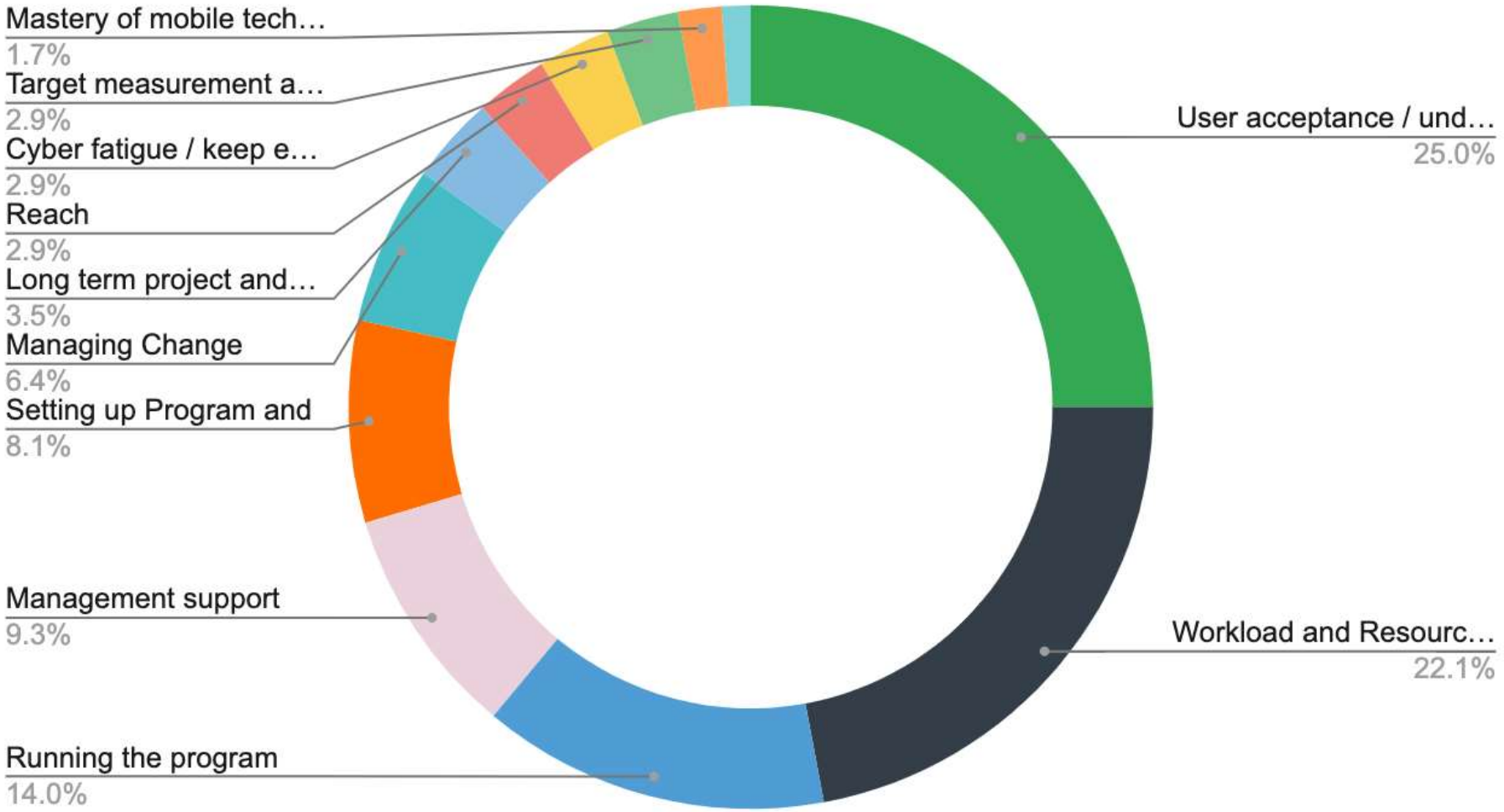
What are the key success factors for a good training



ThriveDX Cybersecurity Awareness Training Study 2022

ThriveDX

Challenges when implementing Awareness



ThriveDX Cybersecurity Awareness Training Study 2022

Get the study!

Thank you!

Meet us or get the full study at

booth 7-301

thomas.reeb@thrivedx.com
andreas.hoberg@thrivedx.com

palo.stacho@securityawareness.guru

Pioneer
SIX GROUP
BOSCH
Technik fürs Leben
Lufthansa
die Mobiliar
Henkel
WÜRTH
OMV
CLARIANT
BÜHLER