/jassics

Cybersecurity Awareness for Everyone

Security is everyone's responsibility

Please don't use your phone during the session!

Sanjeev Jaiswal

Security Awareness Agenda

Security Context

Social Engineering

Spam/Phishing

Password Security

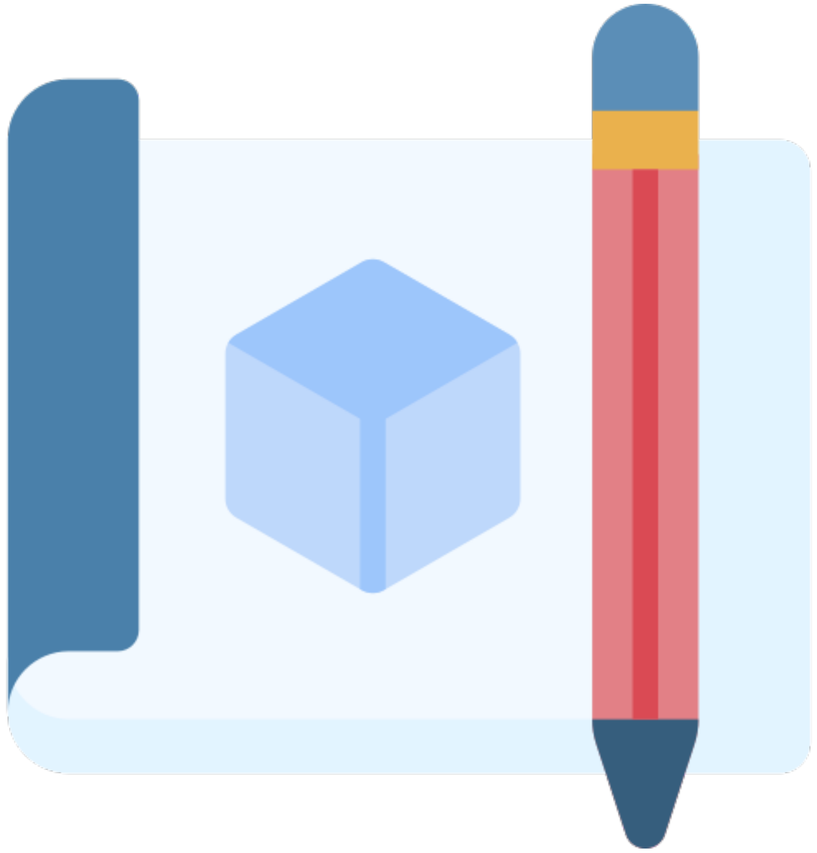
Email Security

Physical Security

Ransomware

Removable Media

Be Compliant



Why Cybersecurity Awareness

It’s all about culture

- Security is everyone’s responsibility
- Learn to protect the organization
- Understand Security Compliance requirements and its importance
- Understand minimal of common security needs for employees
- Helps to secure data from adversaries

Disclaimer

This cybersecurity session to make you aware of

- cyber frauds,
- how it happens,
- how you can avoid and,
- how should you respond.

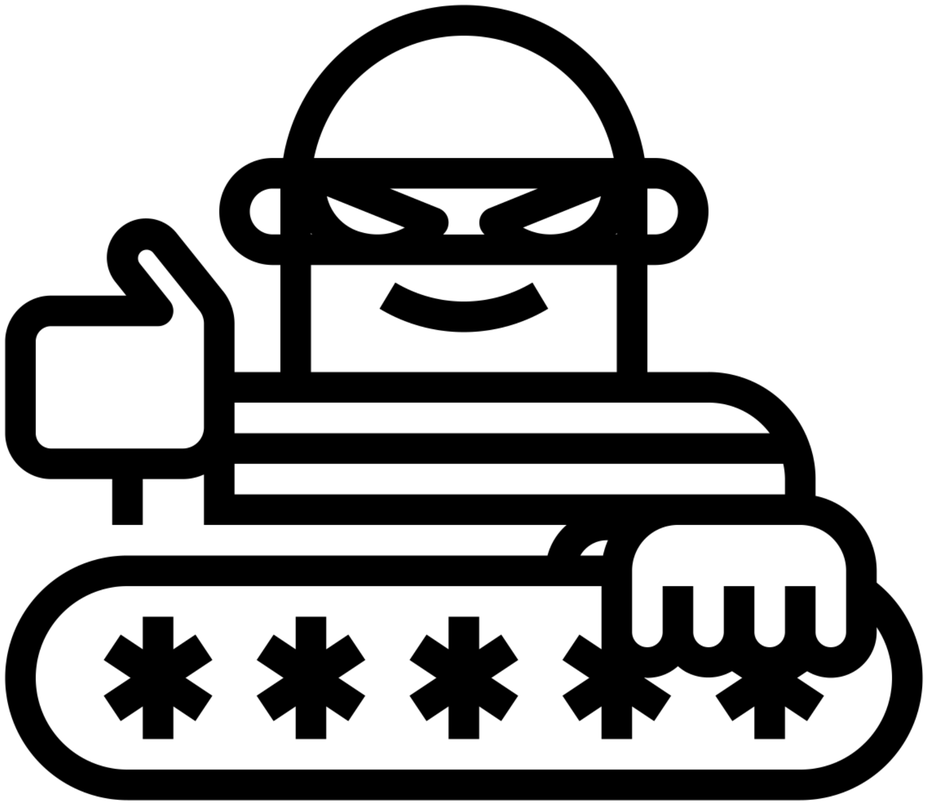
- **Whatever else you do is solely your responsibility!**

Social Engineering

- There is a patch for software vulnerabilities, but not for human stupidity
- Malicious activities accomplished through human interaction
- Uses social interaction to manipulate someone into desired action
- One needs to be aware of when to stop/avoid sharing sensitive information

Social Engineering Techniques

- **Play with emotions to manipulate/get help**
- OSINT: Unknown friend requests
- Spear Phishing: Targeted emails or calls
- Scareware: Help it’s an emergency
- Pretexting: Money scam
- Baiting: Online Frauds
- Pharming: redirection of web traffic from a legitimate site to a fake site
- Dumpster Diving: ATM’s dustbin
- How many of you accept unknown friend request in FB?



Spam and Phishing

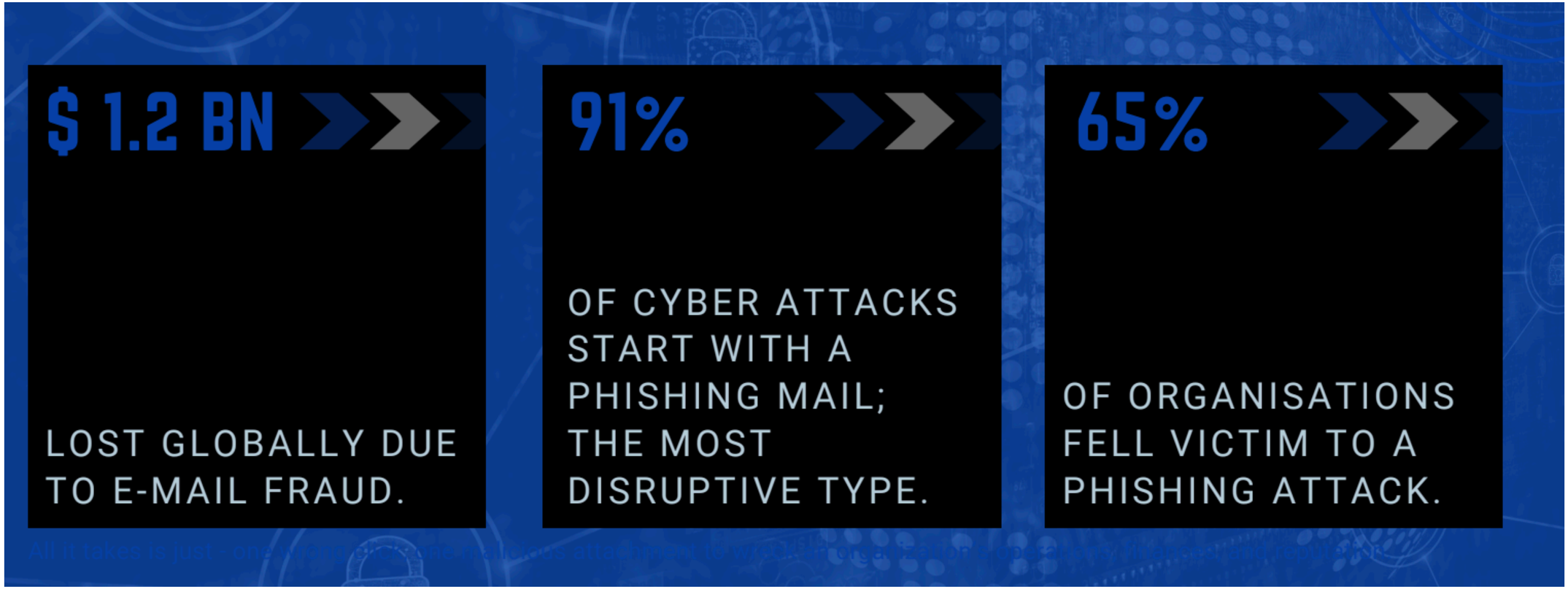
Use your browsing sense

Spam

1. Unsolicited mail or
2. Instant messages or
3. Social Media messages

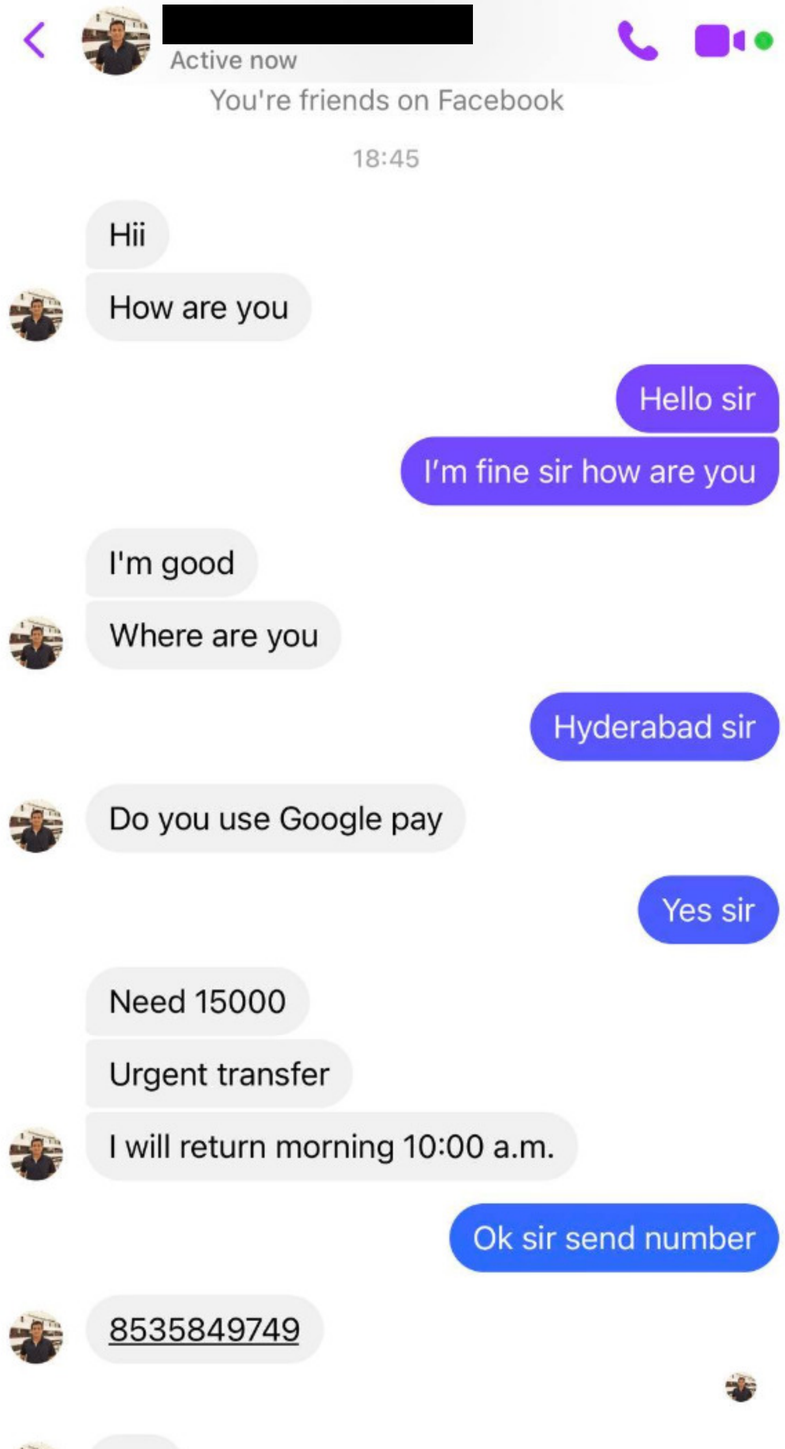
Phishing

1. Email looks from trustworthy resource
2. Mainly to spoof sensitive details

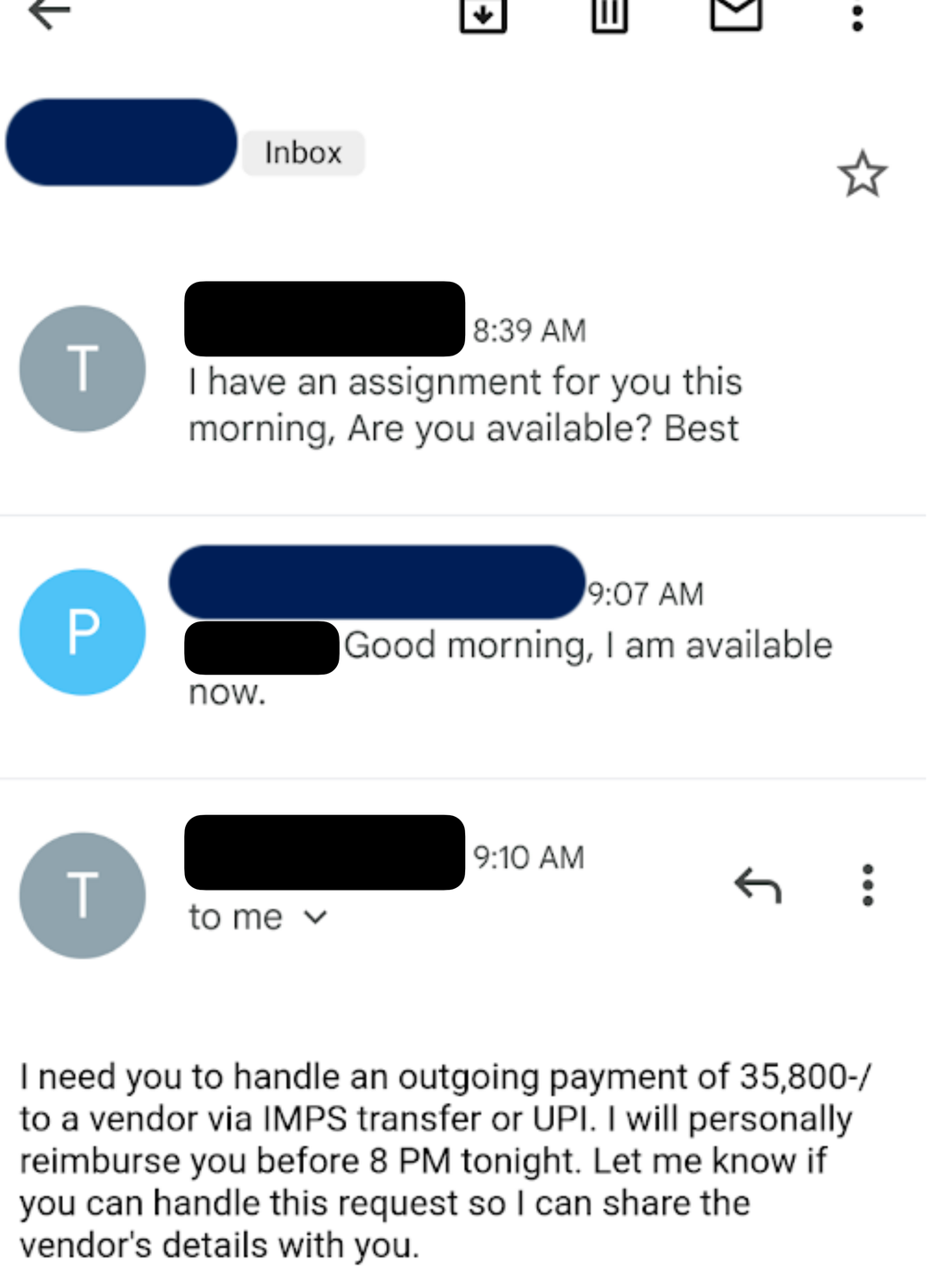

$ 1.2 BN
LOST GLOBALLY DUE TO E-MAIL FRAUD.
91%
OF CYBER ATTACKS START WITH A PHISHING MAIL; THE MOST DISRUPTIVE TYPE.
65%
OF ORGANISATIONS FELL VICTIM TO A PHISHING ATTACK.

How Fraud Happens

Social Media Profile Impersonation



Successful Phishing



---------- Forwarded message ---------
From: [redacted] <yonmmmugmmmih@gmail.com>
Date: Mon, Feb 13, 2023 at 10:13 AM
Subject: On Desk?
To: <[redacted]>

--
Hello [redacted]

Are you be available for a few minutes? I need you to take care of something while I'm in the middle of a conference call meeting. In your response, please include your WhatsApp number.I'm counting on you, this is urgent.

Thanks

Another Phishing Example

Spam or Phishing?

summer internship at [redacted] External Spam ×

Frulloni, Zac <ZFRULL200@caledonian.ac.uk>
to

Wed, 17 May, 19:56 (19 hours ago)

from: Frulloni, Zac <ZFRULL200@caledonian.ac.uk>
to:
date: 17 May 2023, 19:56
subject: summer internship at [redacted]
mailed-by: caledonian.ac.uk
Signed by: caledonianac.onmicrosoft.com
security: Standard encryption (TLS) Learn more

Why is … your inbox.

Rep…

He…

I noticed your company operates a data marketplace and I am writing to express my interest in a summer internship position at [redacted]

As a fourth-year student and soon-to-be Msc in computer science, I am passionate about software development and am eager to apply my skills and experience to an internship opportunity at your esteemed company. I understand that by working at your company I would have the unique opportunity to work with some of the most talented professionals in the field and learn from their expertise.

I have one year of experience working at an IT company where I used Python on a daily basis and am confident that I can make a positive contribution to your team.

I am eager to learn more about the internship opportunities available and to discuss how I can bring value to your team. I look forward to hearing your response. I can forward my CV on your request and look forward to hearing your response.

Kind regards,
Zac

YOU.HAVE.BEEN.PAID jassics,*Check_your_account*_$9571.99💰 Spam ×

jassics admin.78xgckzn32@q0q3tbibyv.us via cofeci.gov.br
to me

from:	**jassics <admin.78xgckzn32@q0q3tbibyv.us>** via cofeci.gov.br
to:	jassics@gmail.com
date:	24 Feb 2022, 00:29
subject:	**YOU.HAVE.BEEN.PAID** jassics,***Check_your_account***_$9571.99💰
mailed-by:	cofeci.gov.br
security:	fundariety.com did not encrypt this message Learn more

Wh … n the past.

Last day

To Claim Your Money

jassics

You've Won jassics,

Please confirm receipt

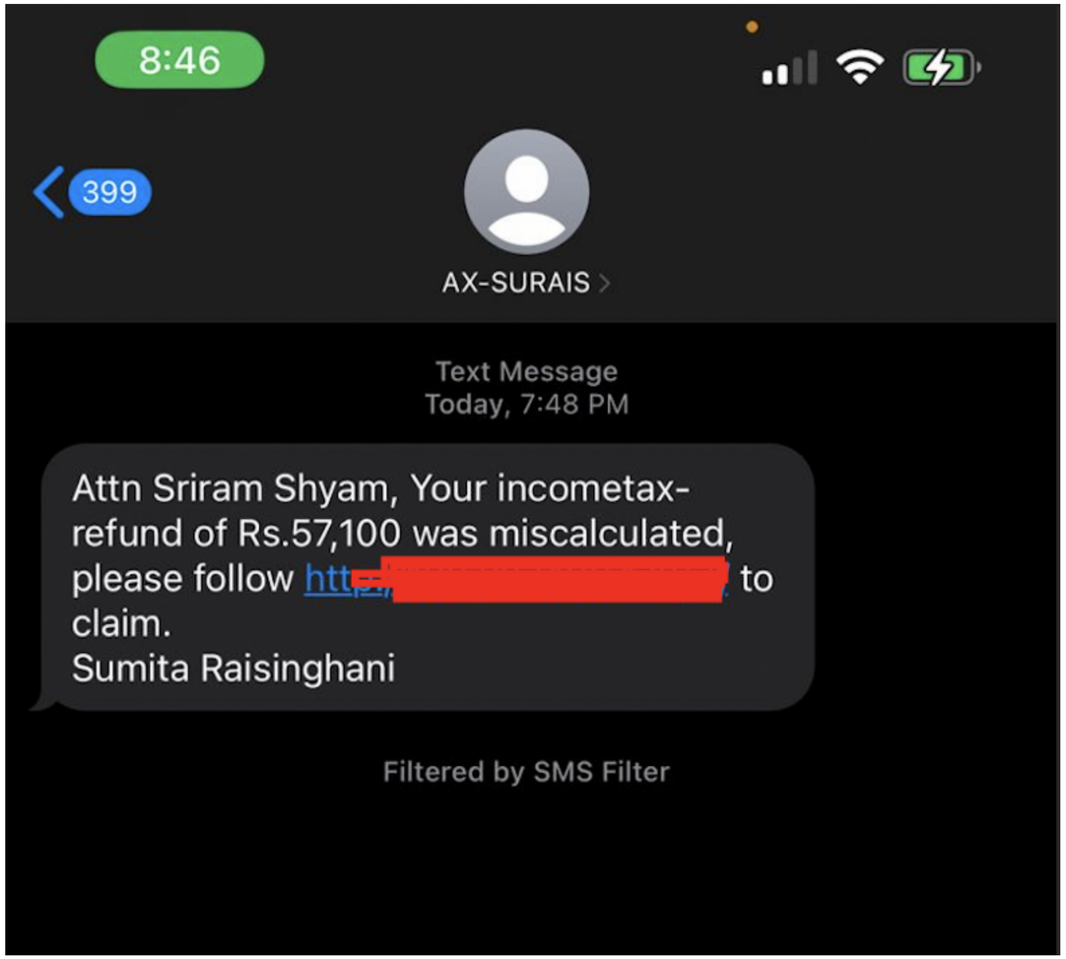
Why it's a spam?

DEAR SBI YONO USER,
Your A/C will be blocked today.update PANCARD for KYC..verify your account login with NetBanking kyc Click https://byrl.me/Bfl3Yl4

Example of Smishing

1. Not a specific username
2. Lots of grammatical mistakes
3. Unrecognised short url
4. Sense of urgency

Few more smashing examples

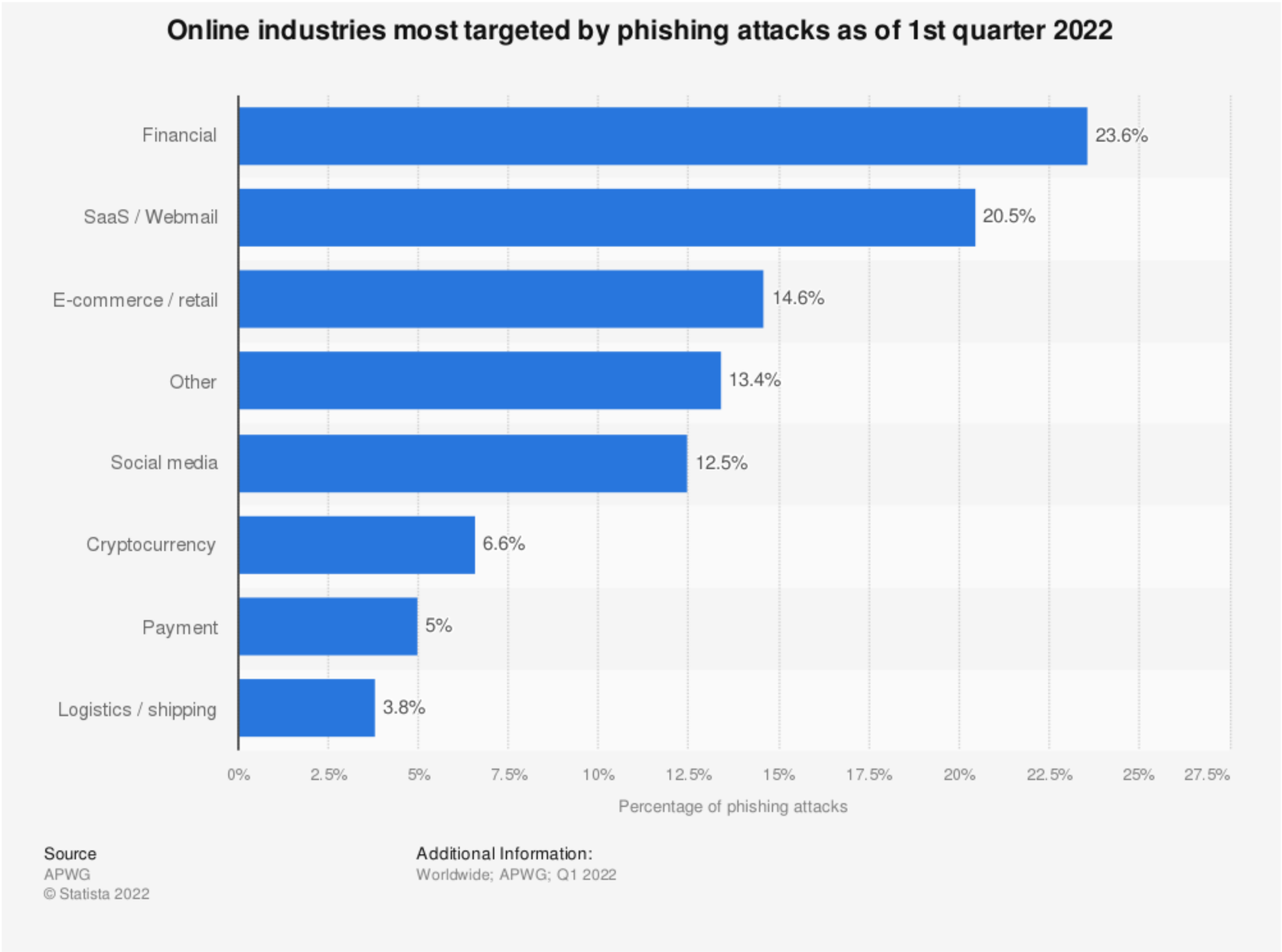


You must be aware of this message and it's not a spam ;)

Never respond to emails/ embedded links in messages/calls asking you to update or verify KYC documents/User ID/Password/ Debit Card Number/PIN/CVV/OTP etc. Immediately change your passwords/CVV/PIN if you have accidentally revealed your credentials.

Spam and Phishing Protection

- Look for
  - “To” email id or To many random mail in “To” field
  - Your Mail id in bcc
- Check for improper grammar and Spelling mistakes
- Sense of urgency: plays with human emotions
- Common greetings
- Ask you to download file
- Change password or share your details from random service with a deadline
- Threat/ultimatum kind of messages


Online industries most targeted by phishing attacks as of 1st quarter 2022
Financial
23.6%
SaaS / Webmail
20.5%
E-commerce / retail
14.6%
Other
13.4%
Social media
12.5%
Cryptocurrency
6.6%
Payment
5%
Logistics / shipping
3.8%
0%
2.5%
5%
7.5%
10%
12.5%
15%
17.5%
20%
22.5%
25%
27.5%
Percentage of phishing attacks
Source
APWG
© Statista 2022
Additional Information:
Worldwide; APWG; Q1 2022

Twilio hacked by phishing campaign targeting internet companies

Carly Page @carlypage_ / 7:28 PM GMT+5:30 • August 8, 2022

But the company said the threat actors seemed undeterred. “Despite this response, the threat actors have continued to rotate through carriers and hosting providers to resume their attacks,” Twilio’s blog post said. “Based on these factors, we have reason to believe the threat actors are well-organized, sophisticated and methodical in their actions.”

TechCrunch has since learned that the same actor also set up phishing pages impersonating other companies, including a U.S. internet company, an IT outsourcing company and a customer service provider, though what impact on these organizations — if any — isn’t currently known.

When reached, Twilio spokesperson Laurelle Remzi declined to say how many customers were affected or what data was accessed by the threat actors. Twilio’s privacy policy says the information it collects includes addresses, payment details, IP addresses and, in some cases, proof of identity.

Twilio said since the attack, it has revoked access to the compromised employee accounts and has increased its security training to ensure employees are on “high alert” for social engineering attacks. The company said it has begun contacting affected customers on an individual basis.

BREACH EXPLAINED

Toyota Suffered a Data Breach by Accidentally Exposing A Secret Key Publicly On GitHub

On October 7th, Toyota revealed a partial copy of their T-Connect source code had been accidentally exposed for 5 years, including access to data for over 290,000 customers.

DWAYNE MCDANIEL

11 OCT 2022 · 4 MIN READ

Share

Forbes

Reddit, the social news and discussion site with 50 million daily users, has confirmed that it has been hacked. In a February 9 security incident posting on the site itself, Reddit said it first became aware of the successful breach of its systems late on February 5. In what it refers to as a " sophisticated phishing campaign that targeted Reddit employees," the incident alert confirmed that the attacker gained access to internal documents and coder, as well as internal dashboards and business systems. However, Reddit also stated that there was no evidence the systems used to run Reddit itself and store the majority of data, the primary production systems in other words, was breached. Furthermore, the ongoing incident investigation has found no evidence that user passwords or accounts were accessed, the report stated.

Targeted employee phishing attack behind Reddit breach

As with all such security incidents, information is currently sparse as the breach investigation continues. However, what we do know is that, also like many such security incidents, the attackers used a targeted phishing campaign to gain access.

Social Engineering Examples

- Example of Phishing with human emotions: https://www.youtube.com/watch?v=lc7scxvKQOo
- How one can break into the company with Social engineering skills: https://www.youtube.com/watch?v=PWVN3Rq4gzw
- Person sneaking everywhere with a ladder: https://www.youtube.com/watch?v=1rTl7_NczK4
- Don’t connect to guest wi-fi or unknown wi-fi: https://www.youtube.com/watch?v=CV39QzFpJx4
- Social Engineering, what’s your password: https://www.youtube.com/watch?v=Pd7x2bHVSAs

Password Security

- Culture for strong password
- Separate password for separate accounts
- Keep your password secret
- Change password periodically
- Don’t choose predictable password(s)
- Avoid Common Password
- Easy to remember, hard to guess
  - Example: Eye-luvu:aa1;)
  - check on. https://password.kaspersky.com/

Weak Passwords and Password Crack Time

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. 12345678
7. 111111
8. 1234567
9. 123123
10. qwerty123
11. 1q2w3e
12. 1234567890
13. DEFAULT
14. 000000
15. abc123
16. 654321
17. 123321
18. qwertyuiop
19. Iloveyou
20. 666666

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years

Email Security

- Don’t share password/sensitive data over plain text: Encrypt it
- Don’t leave your mailbox unattended
- Use official mail id only for official purpose
- Gmail figures out spam and malicious contents, files better
- Internet security tool also provides email security

Ransomeware

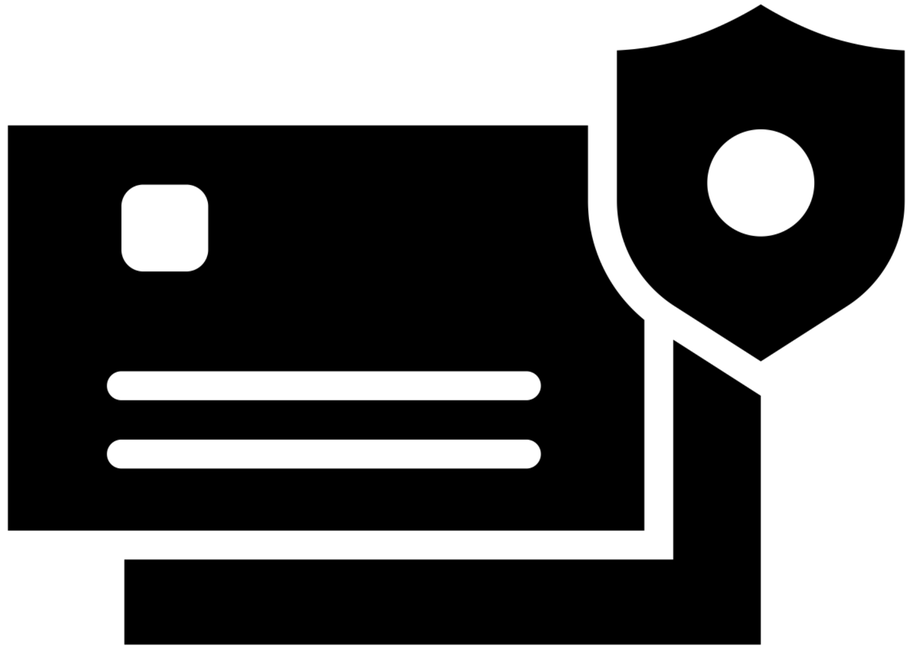
- Game-over, pay now!
- It’s a malicious software that encrypts data until you pay ransom
- Keep anti-virus updated
- Be vigilant with email, files, applications, websites (browsing sense/responsibility)
- Don’t act if you don’t trust

Internet Use

- Check url carefully before opening or clicking
- reliance.com reliance.com (which one is reliable?)
- Input sensitive data only if it has green lock icon. Verify https in url
- Keep your browser up to date
- No P2P downloads
- No porn/gambling websites
- Don’t download unnecessary contents
- Be extra careful when you connect device with unknown network/ wi-fi

Protecting Computer Resources

- Keep Laptop safe wherever you carry
- Don’t use it outside office or home to avoid shoulder surfing, data stealing
- Don’t allow others to use your official devices
- Take proper backup frequently/timely
- Keep system updated
- Don’t use laptop at public places like cafe or airport.



Use of Mobile Device

- Use it with caution
- Keep it password protected at least
- Don’t leave it unattended
- Don’t do any official activities unless it’s approved
- Do whatever is authorised to use in your official phone
- Keep it updated
- Enable cloud backup

Removable Media

- Don’t use removable media unless required and authorised
- Worst case scenario: whole network can be brought down or compromised
- If connected, don’t allow to send anything to the external device
- Need to use it, contact IT Support
- Read Removable Media usage policy

Social Media Policy

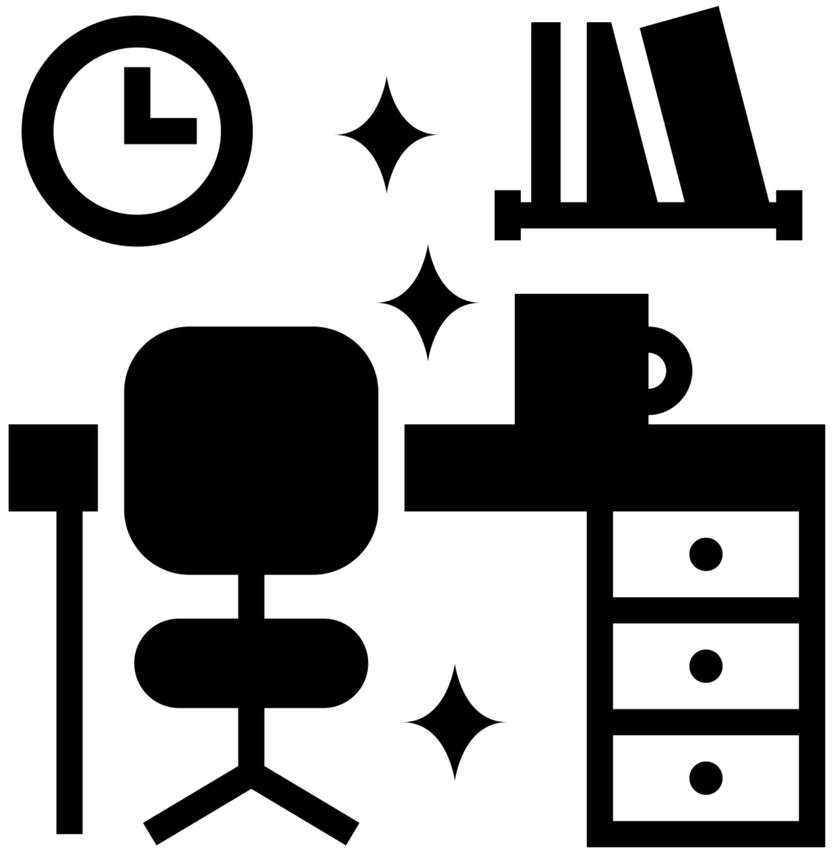
- Share with a responsibility
- Don’t indulge with political debate over social media
- Don’t discuss about company data unless it’s public
- Sharing publicly which should be within company only
- Offensive posts intentionally to harm someone’s reputation
- Posts that can create hostile environment

Physical Security

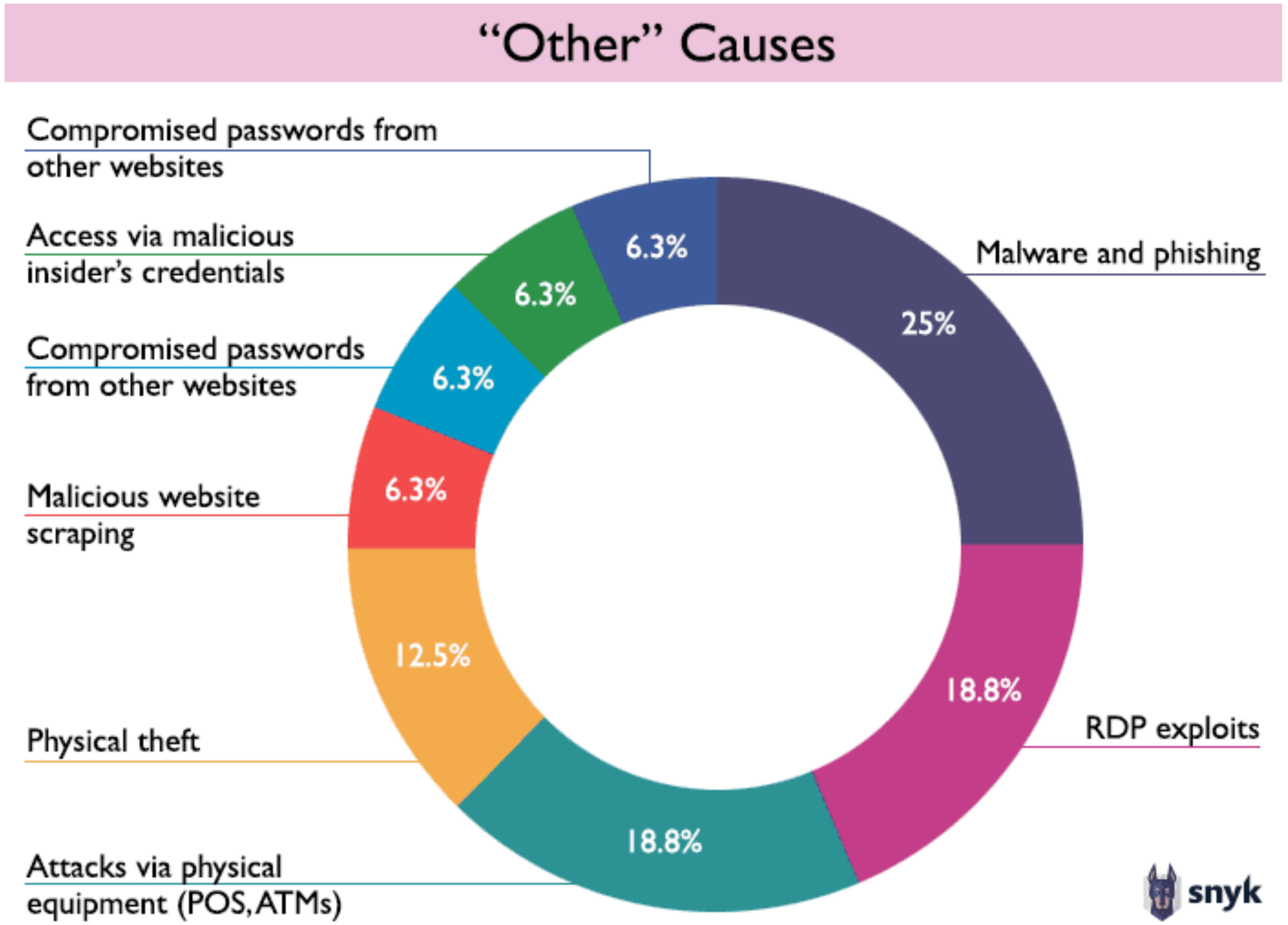
- No Tailgating, show ID card, fingerprint etc. for audit and tracking purpose.
- Unusual piggybacking, please report
- Question all strangers, alert guard or management
- It’s our responsibility to make our premise safe and secured.
- Use only authorised places
- Report misuse of any physical infra
- Use only given access point(s)
- Use shareable items carefully and don’t damage either urself or the equipment ;)

Clean Desk

- Let’s not write over the desk
- No sensitive info displayed
- Don’t leave your mobile or laptop unattended
- Don’t write sensitive information on paper and paste it on desk
- Check properly before leaving the desk or leaving for the day.
- If needed, use lockable storage
- Possibly use cafeteria for eatery purpose
- Use shredder to destroy sensitive paper documents

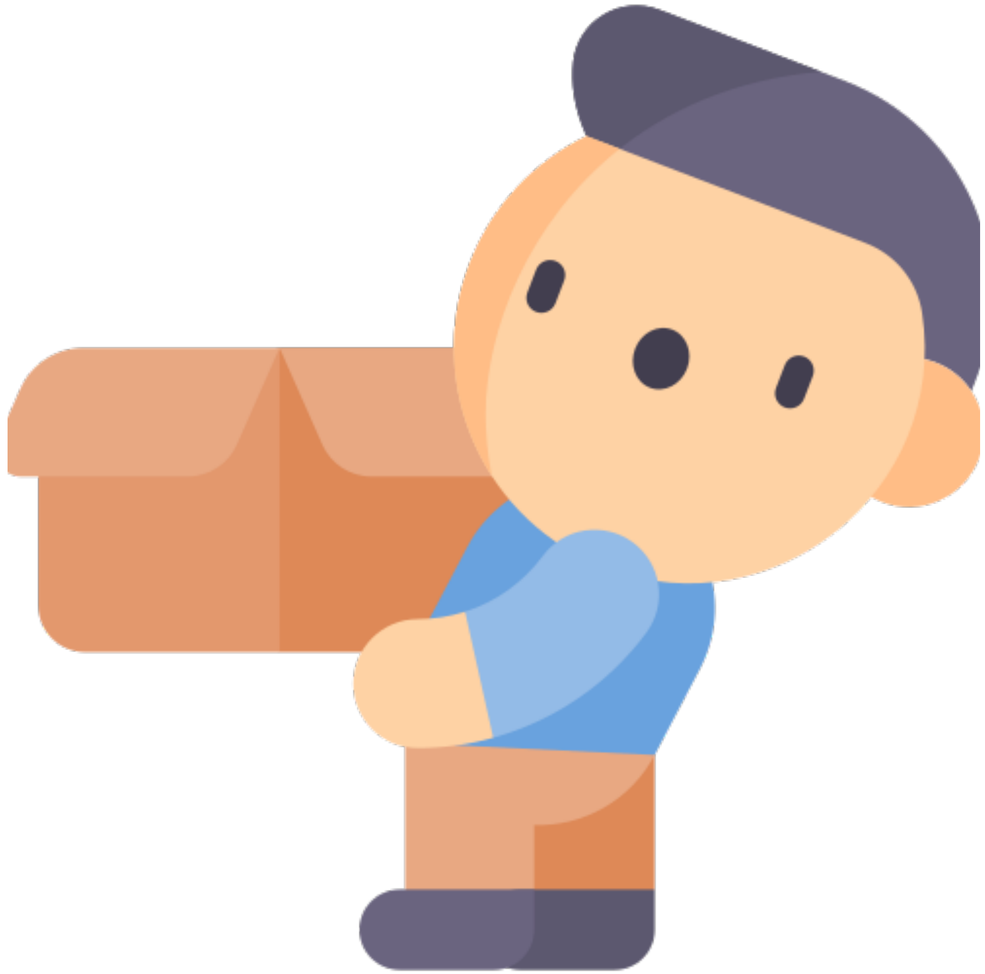


Data Breaches Reasons



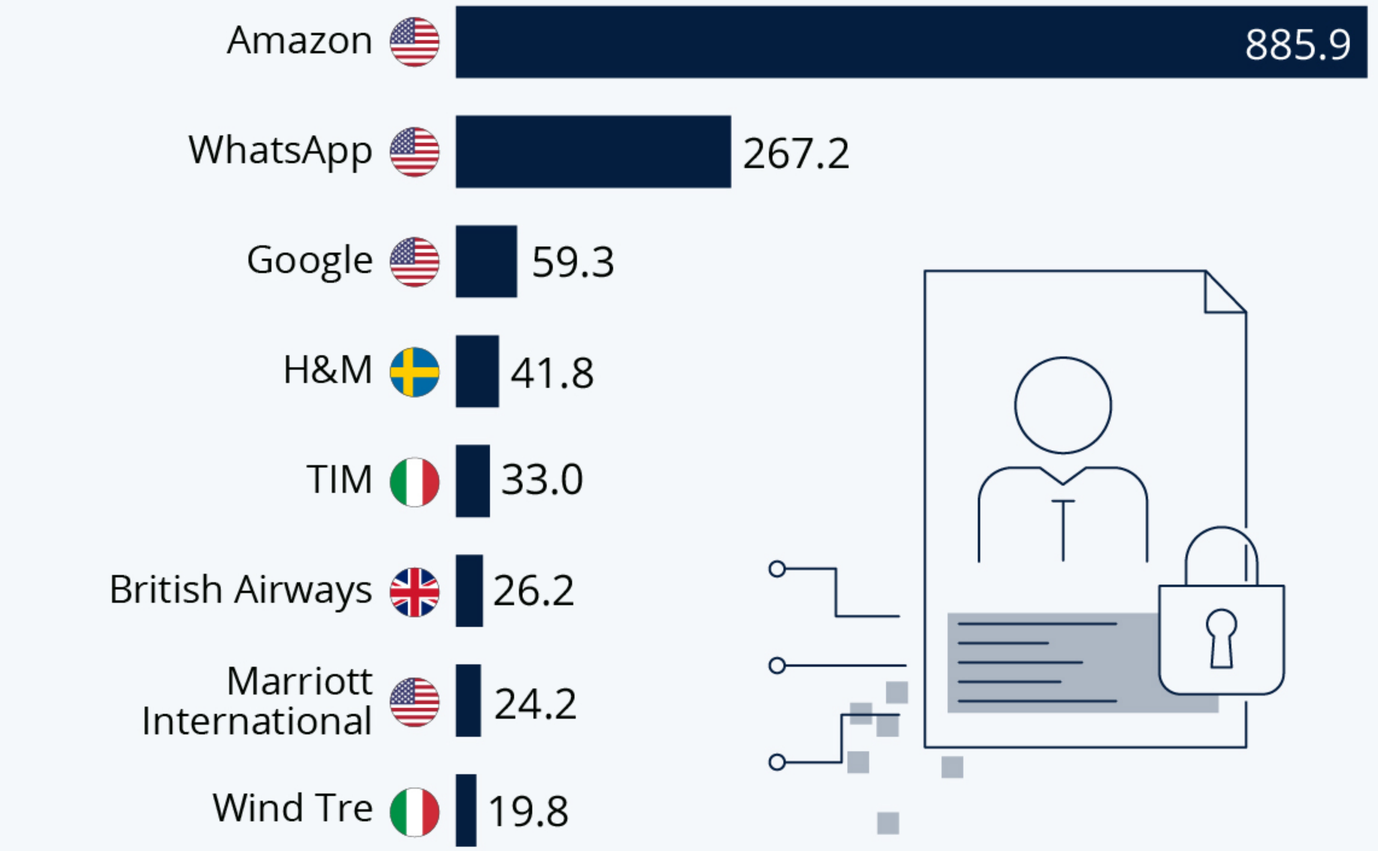
Be Compliant

- Do what’s allowed and be compliant
- No Weak Passwords please!
- Don’t share password to anyone
- Use only approved software
- No tailgating
- Inappropriate Dress Code
- Follow official policies and guidelines
- Reach out to HR or Compliance team for any issues.



Big Tech, Big Fines

Highest fines for breaching one or more articles of the GDPR (in million U.S. dollars)



Source: CMS GDPR Enforcement Tracker

Incident Response

- Any deviation from usual activities
- Ex: internet goes down now and then, sudden unusual traffic to website, unattended printouts, usb or anything
- Unusual conversation inside/outside with known/unknown folks
- Suspicious calls, messages, mails etc.
- Lifesight sensitive data is public
- Any malpractices or wrongdoings
- Read whistleblower policy and code of business conduct and ethics carefully.
- Suspicious or foul activities, mail to security team immediately.

Summary

- Keep system updated
- Follow Clean desk
- Share the info, docs carefully anywhere
- Avoid the damage from malware
- Don’t fall prey of phishing scam
- Be a good Samaritan, help us to improve Compliance and security.
- Prevent unauthorised access from known or unknown people
- Be compliant

Stay alert, be safe

Follow me for more contents on cybersecurity

Linkedin: https://www.linkedin.com/in/jassics/
Twitter: https://twitter.com/jassics
GitHub: https://github.com/jassics