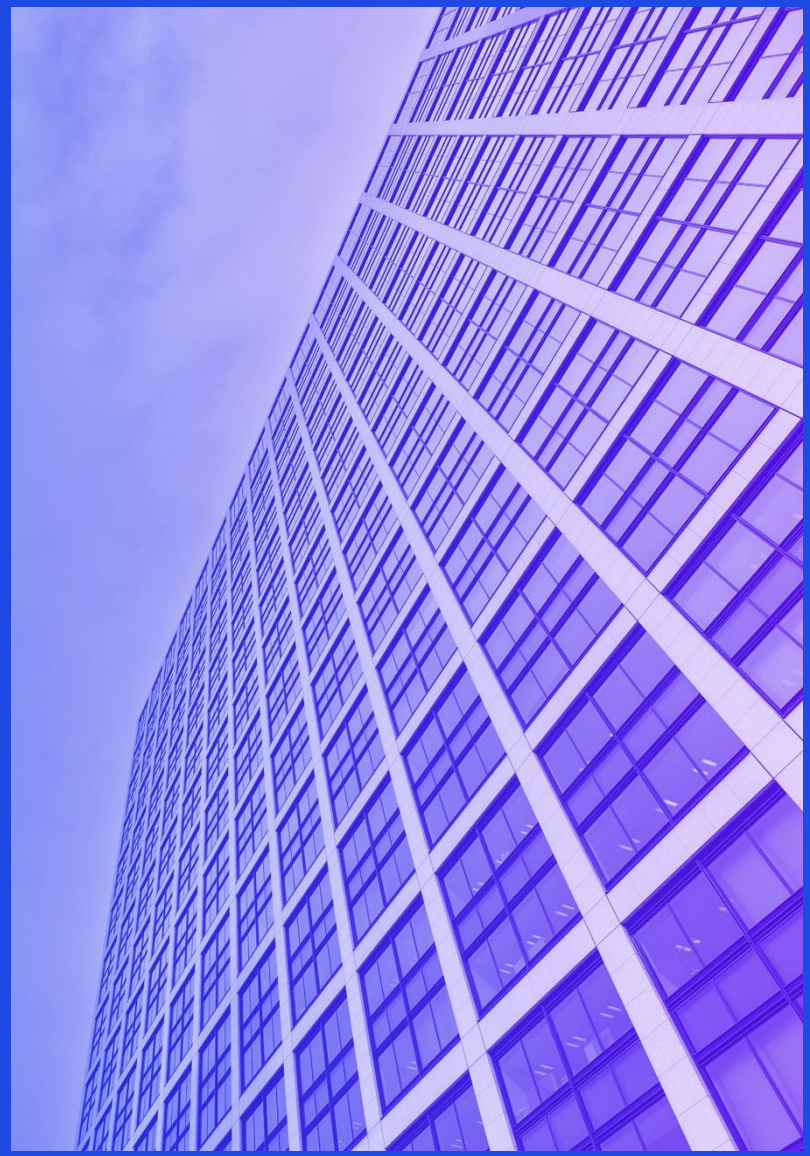
# Cyber awareness session



**Presented by**

**Ravi Sankar**

**Head of Cyber and Technology Consulting**

**KPMG in Caricom**

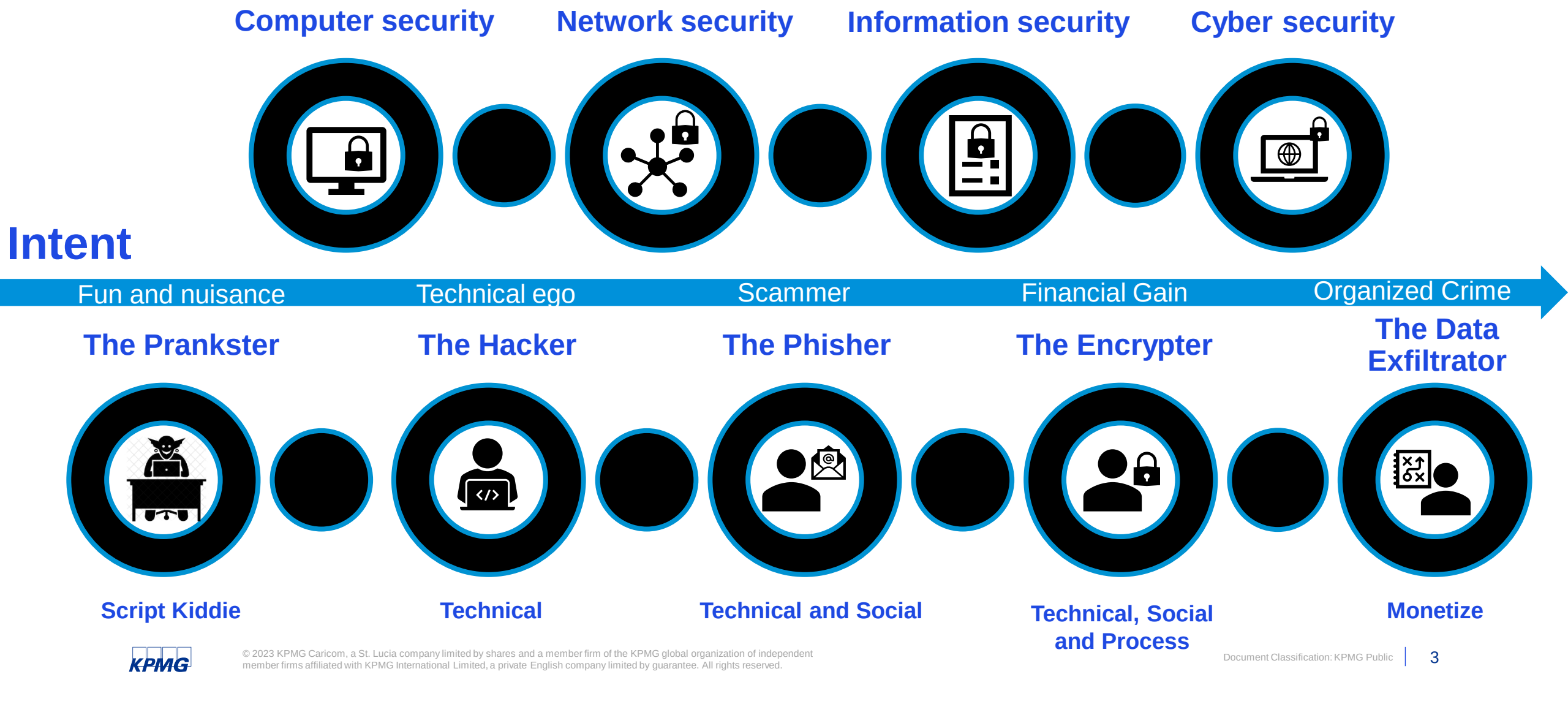
—

June 23, 2023

# Why are we here today?

1. It matters to you and to your business
2. What we need to do, to stay relevant
3. World is changing and only the fittest and resilient will survive

# The Big Shift – Evolution of Cyber Security



# Cyber crime – today

**43%** of C-Suite business leaders who reported a data breach cited human error as the second major cause

**148%** Increase in ransomware attacks

**311%** Increase in ransom amounts since 2019

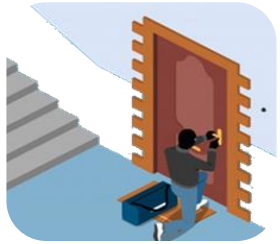
**10.5 tr** Global cyber crime damages worth in USD by 2025

# Cyber crime mimicking physical crime

**Physical Crime**

**Chances of Monetization = Low**

**Chances of Getting Caught = High**



Robbery

Stealing money

Bombing

Kidnapping for ransom

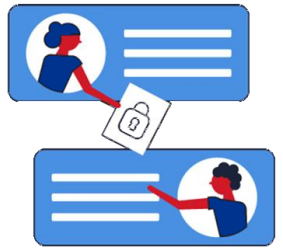
**Cyber Crime**

**Chances of Monetization = High**

**Chances of Getting Caught = Low**


Confidential Information leakage

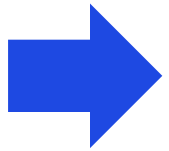
Account hacked for financial attack



Denial of service

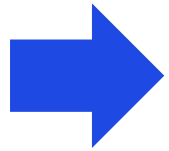
Ransomware

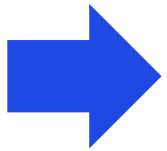
# The future – attacks moving from …



**Individual corporation** to **Ecosystems of corporations**

**Corporations** to **Homes**





**Homes** to **Privileged Users**

# Cyber threats in the current landscape

**Recent cyber security** incidents which have had far reaching consequences



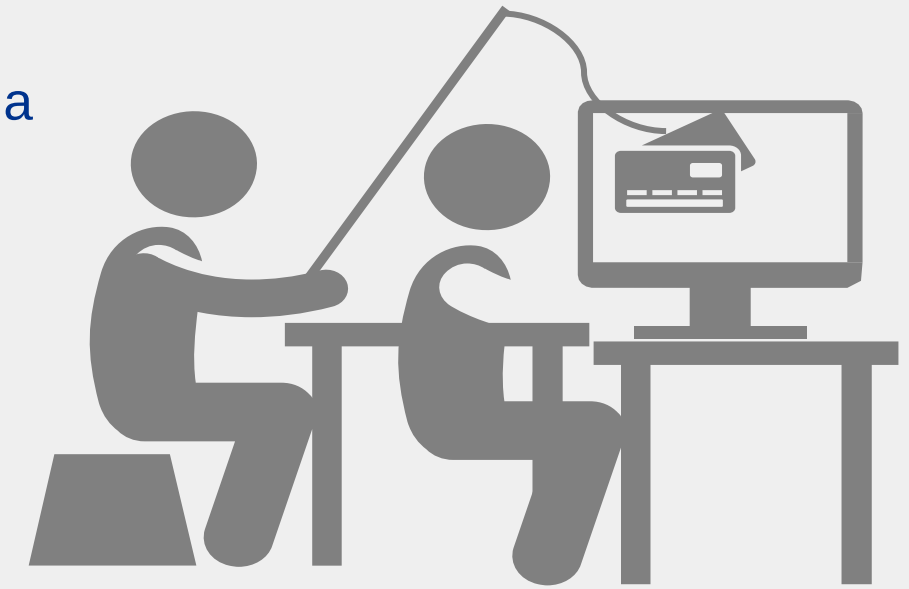
# Cyber Security in the last week

## Top Stories

- Jimbos protocol hack results in loss of $7.5 million worth of assets
- Top aviation company Safran Group left itself vulnerable to cyberattacks, likely for well over a year
- Financial institution in Jamaica hit with a cyber attack in the past two weeks
- Italy's Industry Ministry reports “heavy” cyberattack
- 328,000 IDs feared stolen in “sophisticated” Latitude Financial hack
- LockBit ransomware claims Essendant attack, company says “network outage”
- Brazilian hackers target Portuguese financial institutions
- New England-based health insurer says patient data was stolen in ransomware attack
- Insurance Information Bureau of India suffers ransomware attack by Russian hackers

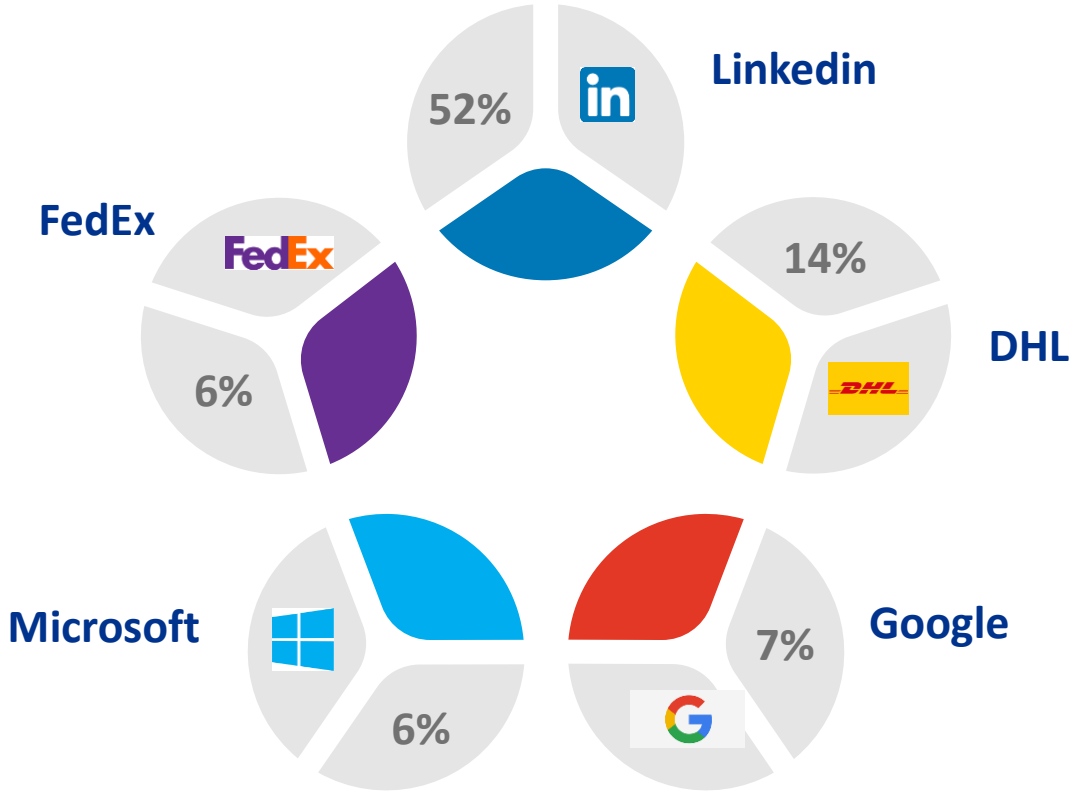
# Typical attacks – Phishing ( 70% Global attacks start here)

- Spear or Targeted (Whale Phishing)
- Attachments and Account Access
- Also, fraudsters are imitating a hotline, asking to “confirm” confidential information.
- AI is now being used to impersonate persons



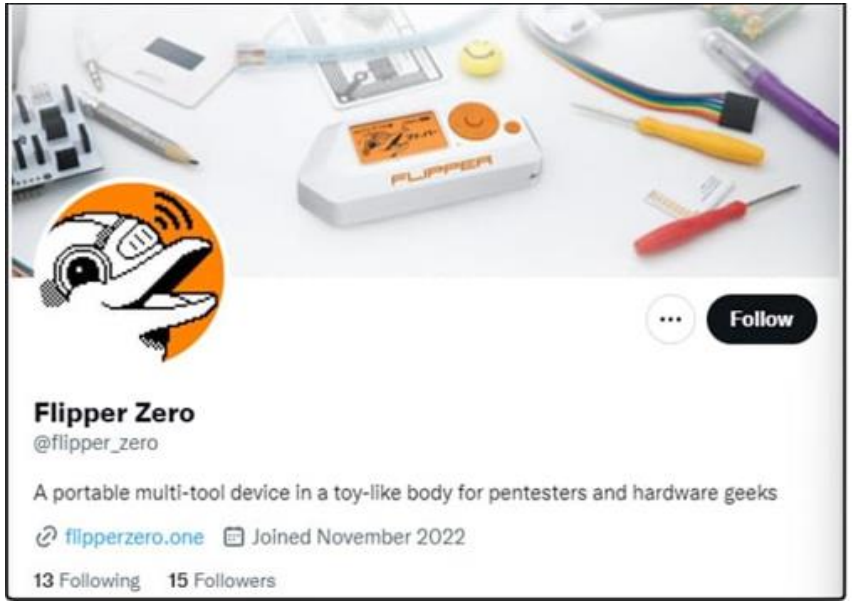
# Global Phishing Statistics

In Q1 of 2023, phishing emails using LinkedIn the most imitated brand for phishing attempts globally. This is followed by Google, Microsoft and DHL.

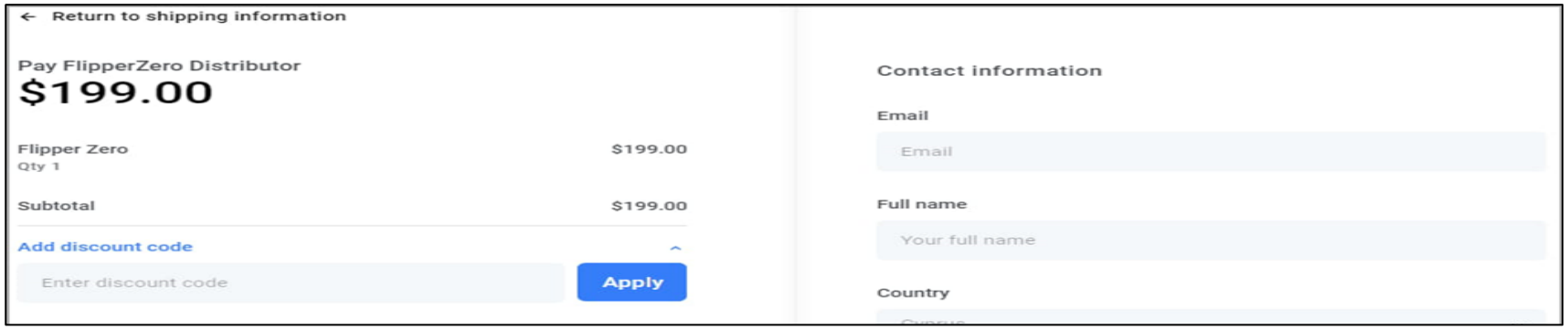


# Phishing or real?

**With the advent of technologies such as ChatGPT, phishing scams are becoming more realistic in nature.**








## Spot the difference

- Popular phishing scams replicate the style, writing and format of the target account
- ChatGPT can instantly produce grammatically correct and natural-looking writing, which would resolve one the biggest challenges that scammers face when creating their baits.

# WhatsApp scam

**WhatsApp's two billion users send an average of 100 billion messages every day. WhatsApp has become a means of choice for fraudsters distributing scam messages**

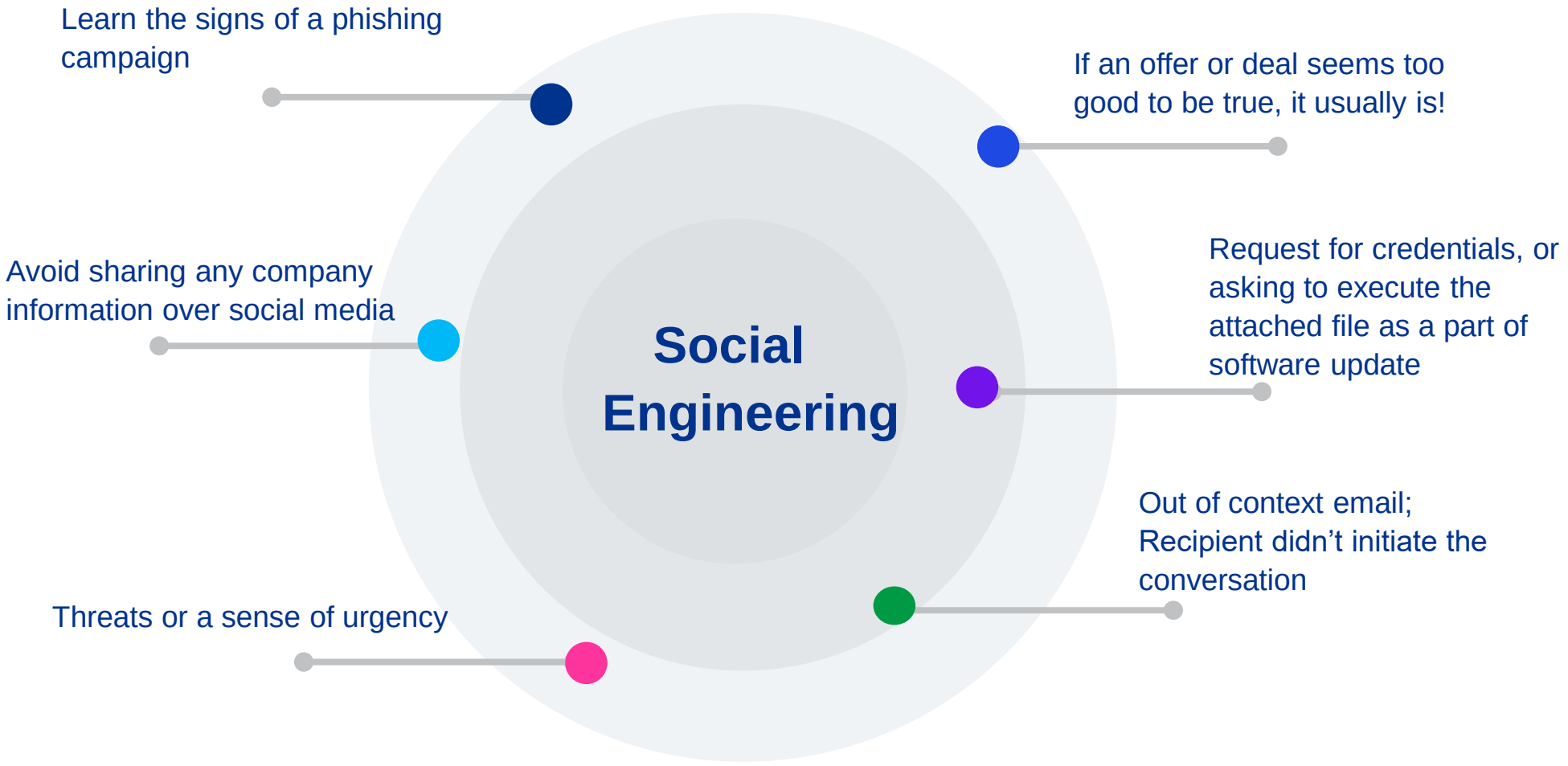
## Types of WhatsApp Scams

1. **Voicemail hacking:** Cybercriminals gaining access to a user's WhatsApp account by breaking into their voicemail box to obtain their verification code
2. **WhatsApp hijacking:** Hijacker obtains the user's phone number. They install WhatsApp on their own device and then contacts the victim, requesting a verification code for the victim's account
3. **Impersonation scams:** Involves the scammer pretending to be a friend, family member, or acquaintance, contacting a user from an unknown number (although the profile picture may be familiar) urgently
4. **Malicious links:** External links are a simple scam method for fraudsters, enabling mass distribution of a URL that leads to the recipient being directed to a browser

## 2022 – Rediroff.com scam

- Takes advantage of external links that typically start with Rediroff.com or Rediroff.ru.
- These links are spread and circulated unknowingly by the WhatsApp community.
- The links are often masked by a "click here to claim your prize" message, so users may not even see the actual URL.
- Once clicked, the Rediroff.com link opens a phishing site promising grand prizes to the recipient if they follow specific tasks that make fraudsters heaps of money.

# How to defend yourself



# Cybersecurity and privacy for accounting firms

**Data Protection:** Accounting firms deal with vast amounts of financial and personal data. Implement strong data protection measures, such as encryption, access controls, and secure storage, to safeguard client information from unauthorized access or breaches.

**Employee Awareness and Training:** Train employees on cybersecurity best practices, such as recognizing phishing attempts, using strong passwords, and following secure data handling procedures. Regularly reinforce these practices to promote a security-conscious culture within the firm.

**Secure IT Infrastructure:** Maintain a robust and up-to-date IT infrastructure that includes firewalls, intrusion detection and prevention systems, antivirus software, and regular patch management. Conduct regular vulnerability assessments and penetration testing to identify and address potential weaknesses.

**Secure Remote Access:** With the increasing trend of remote work, ensure that remote access to the firm's systems and data is secure. Implement secure Virtual Private Network (VPN) connections, multi-factor authentication, and endpoint security solutions to protect against unauthorized access.

**Client Data Sharing:** When sharing sensitive client data, use secure channels, such as encrypted email or client portals, to maintain confidentiality. Implement access controls and permissions to ensure that only authorized individuals can access and share client information.

**Incident Response and Business Continuity:** Develop an incident response plan that outlines steps to be taken in the event of a cybersecurity incident or data breach. This plan should include procedures for notifying affected parties, preserving evidence, and restoring operations. Regularly test the plan to ensure its effectiveness.

**By prioritizing cybersecurity and privacy, accounting firms can protect client data, maintain trust, and mitigate the risks associated with cyber threats and data breaches. It's essential to regularly review and update security measures to stay ahead of evolving cyber threats.**

# Cybersecurity and privacy for accounting firms

**Regulatory Compliance:** Stay abreast of relevant data protection regulations and compliance requirements, such as the General Data Protection Regulation (GDPR) or the similar regional Acts. Implement necessary controls and processes to ensure compliance with these regulations.

**Vendor Management:** Assess the security practices of third-party vendors that have access to the firm's data or systems. Conduct due diligence on their security controls, data protection measures, and incident response capabilities to mitigate potential risks.

**Regular Security Assessments:** Engage external cybersecurity experts to conduct periodic security assessments and audits of the firm's systems, networks, and processes. These assessments can help identify vulnerabilities and provide recommendations for improvement.

**Privacy Policies and Consent:** Develop clear and transparent privacy policies that outline how client data is collected, stored, and used. Obtain appropriate consent from clients regarding the collection and processing of their personal information.

**By prioritizing cybersecurity and privacy, accounting firms can protect client data, maintain trust, and mitigate the risks associated with cyber threats and data breaches. It's essential to regularly review and update security measures to stay ahead of evolving cyber threats.**

# Future of cyber threats

As cyberattacks increasingly take a toll on corporate bottom lines and reputations, cyber security threats are evolving and rapidly changing.

# Future of cyber security threats

Key Loggers

Ransomware


**Intercepts OTP codes** banks sent to users via SMS or push notifications. Can bypass some of the 2FA solutions employed. Sends the code to criminals to bypass logins and authorize fraudulent transactions.


**Infiltrates system without users consent** – it is distributed via spam emails (Windows OS, private messages, SMS, Skype) and malicious websites


**Remote Administration Tool (RAT) gives control to remote users** on administration of your computer. Covid19 campaigns have been distributing a large number of RAT tools to users.

# Hacker definition changing . . .

## YESTERDAY . . .

**Bad "actors"**
- Isolated criminals
- "Script kiddies"

**Targets**
- Identity theft
- Self-promotion opportunities
- Theft of services

**Target of Opportunity**

## TODAY . . .

**Bad "actors"**
- Organized criminals
- Nation states
- Hacktivists
- Insiders

**Targets**
- Intellectual property
- Financial information
- Strategic access

**Target of Choice**

# The attacks are easy

Sophisticated tools that compromise your browser on desktop, laptop or mobile.

# What am I hinting at?

Your digital asset was a lot safer when you were in office.

At home, while personal security is addressed, safety of the **digital assets is your responsibility** from a logical and physical perspective.

# Data Privacy- What is it?

**Data privacy refers to the protection and control of an individual's personal information or data, ensuring that it is collected, used, and shared in a way that respects their rights and maintains their confidentiality.** It involves the right of individuals to determine when, how, and to what extent their personal data is collected and processed by others, such as organizations or governments.

Data privacy encompasses various aspects, including:

- Data Collection: including IP addresses ( persons visiting your website)
- Data Storage and Security
- Data Processing and Use:
- Data Sharing and Transfer
- Individual Rights

**Data privacy is essential for maintaining trust in the digital age**, as it helps protect individuals from identity theft, unauthorized surveillance, and unwanted marketing practices. By safeguarding personal information, individuals can exercise greater control over their online presence and make informed decisions about the use of their data**.**

# How much is your identity worth on the black market?

**Personal Identity**

**$2 USD**


**Government ID**

**$ 30 USD**


**Online Bank Creds**

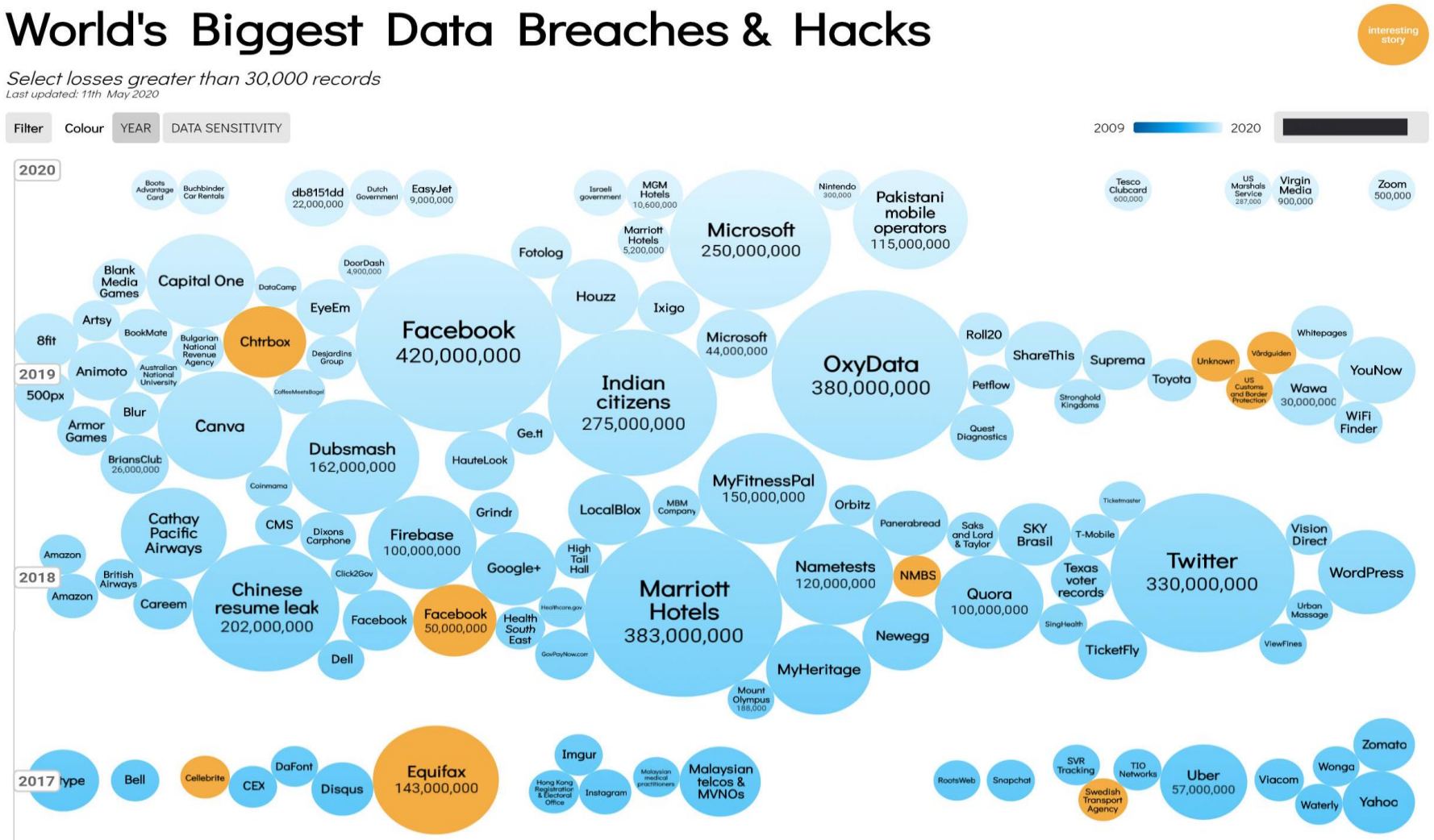
**$ 500 USD**


**PayPal /Ebay**

**$ 300 USD**

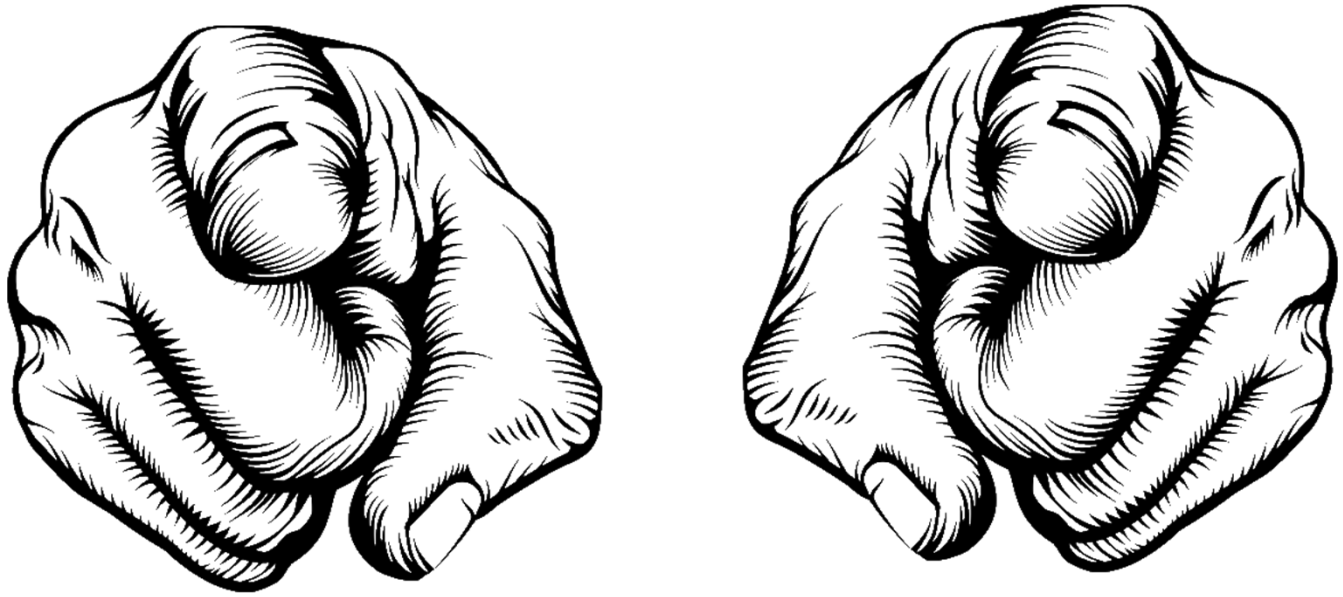
Source: https://www.pacetechnical.com/much-identity-worth-black-market/

# Data breach statistics




**Source:**
https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

# Our biggest threat to data privacy



**Simple steps individuals can take to prevent data breaches:**

- Use strong passwords
- Encrypt sensitive information
- Keep software up to date
- Be cautious about sharing personal data online

**KNOW YOUR DATA AND WHERE IT LIES:**

# How KPMG can help you on your cyber and privacy journey

**Cybersecurity Strategy and Governance:** KPMG can assist in developing a comprehensive cybersecurity strategy and governance framework tailored to your organization's needs. This includes assessing risks, defining security objectives, and establishing policies, procedures, and controls to protect your digital assets.

**Cyber Risk Assessment and Management:** KPMG can conduct a thorough assessment of your organization's cyber risks and vulnerabilities. They can help identify gaps in your security posture, evaluate potential impacts, and recommend risk mitigation strategies to enhance your cyber resilience.

**Privacy Compliance:** KPMG can assist with privacy compliance efforts, such as implementing frameworks aligned with global privacy regulations (e.g. GDPR, JDPA, BDPA), conducting privacy impact assessments, developing data protection policies, and establishing privacy governance structures.

**Incident Response and Recovery:** In the event of a cyber incident, KPMG can provide support in incident response and recovery. They can help investigate the incident, contain the breach, restore systems, and assist with communication and remediation efforts to minimize the impact on your organization.

**Security Architecture and Technology Enablement:** KPMG can help design and implement robust security architectures and technology solutions tailored to your organization's needs. This includes evaluating and selecting security technologies, designing secure networks, and implementing security controls and monitoring capabilities.

**Cyber Awareness and Training:** KPMG can assist in developing cybersecurity awareness and training programs for your employees. They can provide training on best practices, conduct phishing simulations, and create customized awareness materials to educate your workforce on cyber threats and prevention measures.

**Third-Party Risk Management:** KPMG can help you assess and manage the cybersecurity risks associated with third-party vendors and suppliers. They can conduct due diligence assessments, develop risk management frameworks, and establish vendor security assurance programs to ensure the security of your supply chain.

**Cybersecurity Maturity Assessments:** KPMG can evaluate your organization's cybersecurity maturity level through comprehensive assessments. They can benchmark your security practices against industry standards, identify areas for improvement, and provide recommendations to enhance your overall cybersecurity posture.

These are just a few examples of how KPMG can support you on your cyber and privacy journey. It's important to engage with KPMG directly to discuss your specific needs and tailor their services to your organization's requirements.

# Q&A

**kpmg.com/socialmedia**



**Document Classification: KPMG Public**