FOURTH COMMAND

CYBER DEFENSE

CYBERSECURITY & CHALLENGES 2020-30

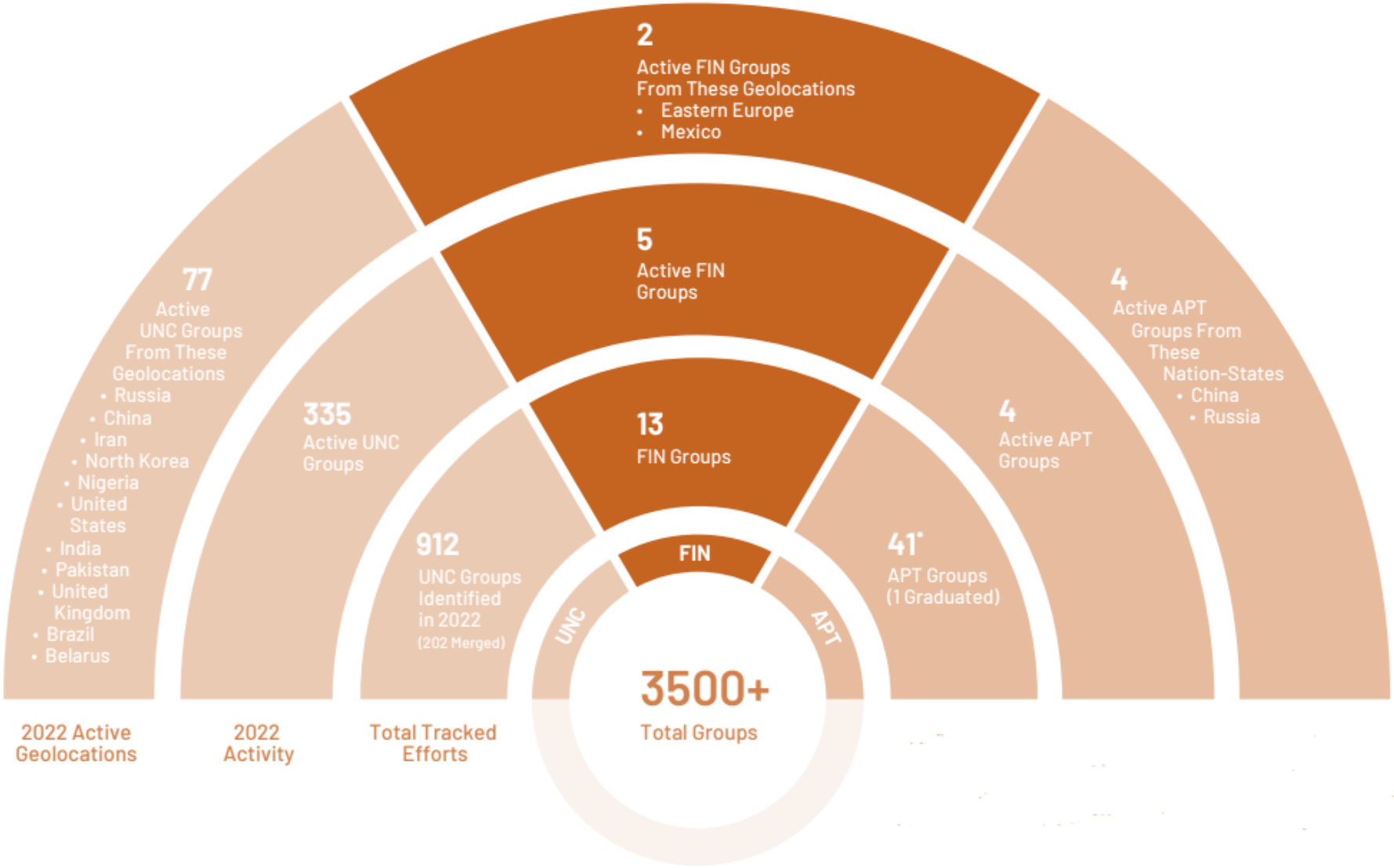
ANSHUL PAREEK


MIDDLE EAST CYBER THREAT
LANDSCAPE
WORLD WAR CYBER

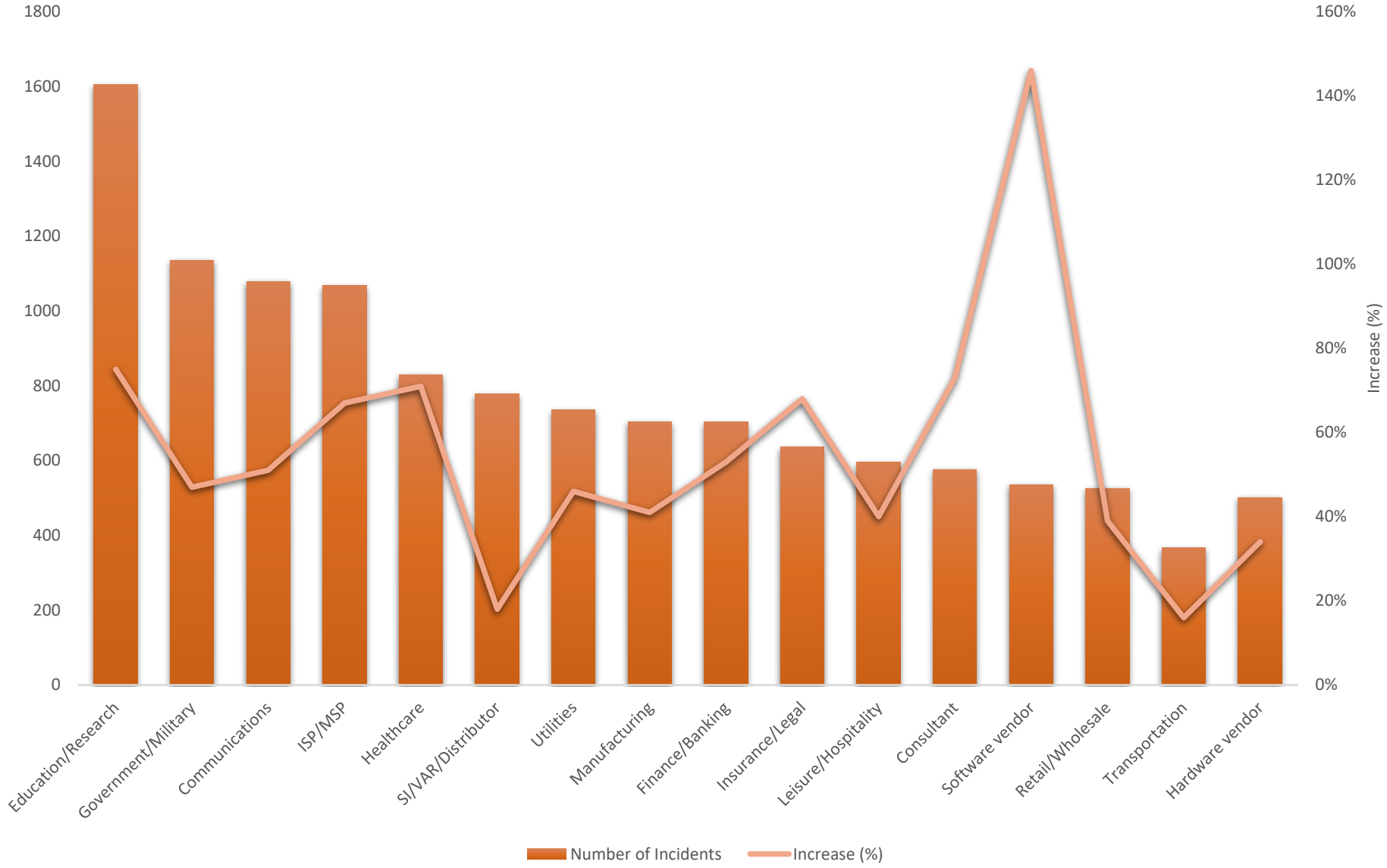
INCREASING CYBERSECURITY LANDSCAPE

- **Increasing digitalization and reliance on technology**
  - Growing economies and government initiatives
  - Smart city initiatives
- **Rising cybercrime threat**
  - Sophistication of cyberattacks
  - High-profile cyberattacks
- **Regulatory landscape and government support**
  - Stricter data privacy regulations
  - Government cybersecurity initiatives
- **Other contributing factors**
  - Increased awareness of cybersecurity risks
  - Maturing cybersecurity market

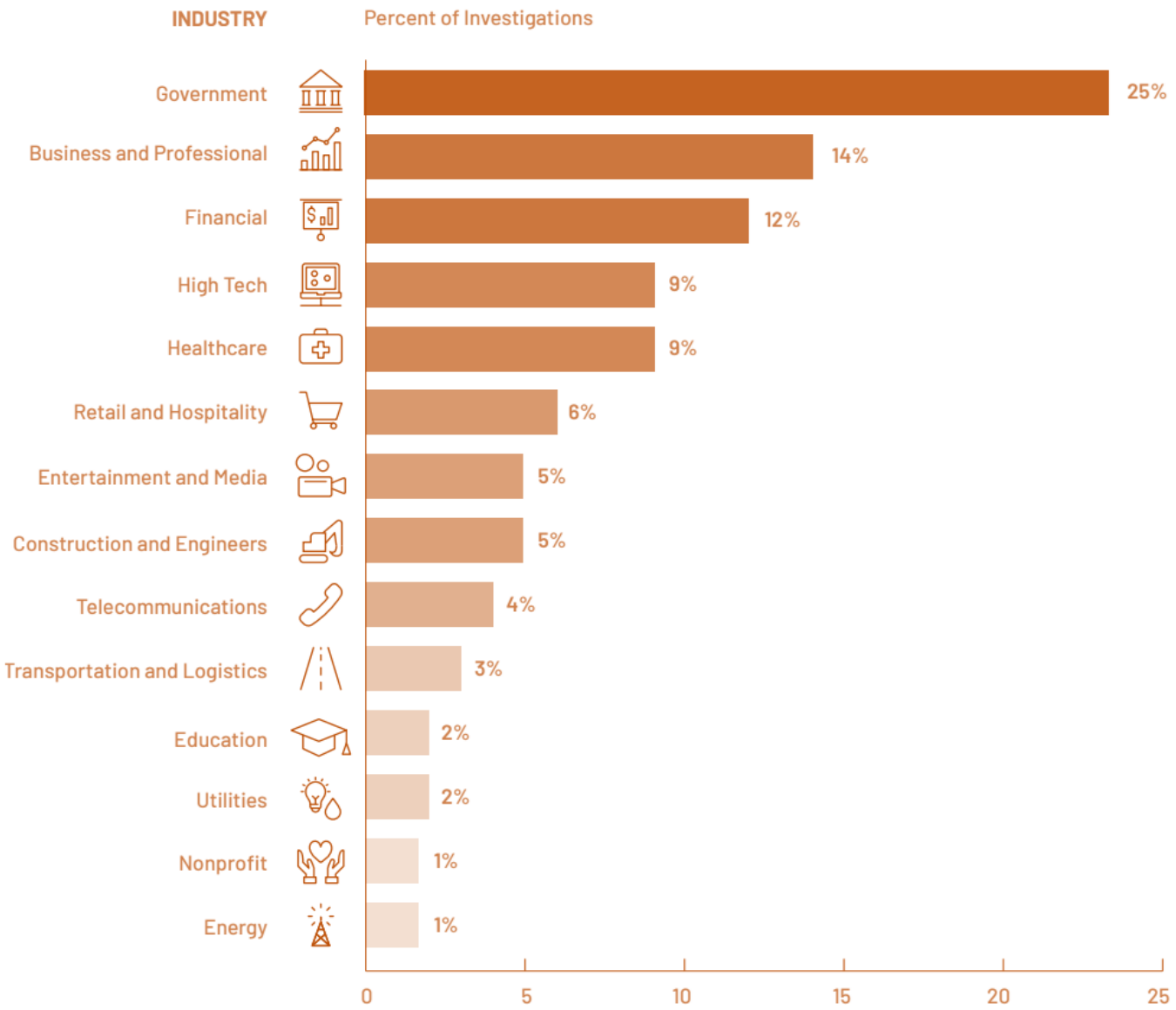
THREAT ACTORS



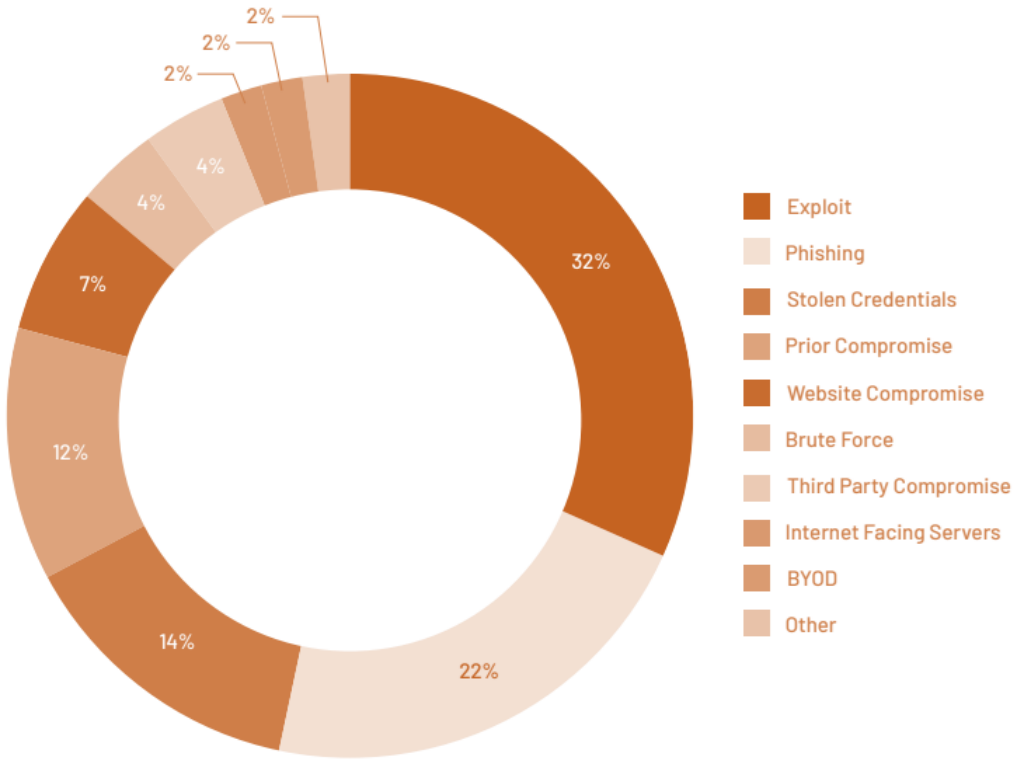
AVERAGE WEEKLY ATTACK PER INDUSTRY/ORGANIZATION



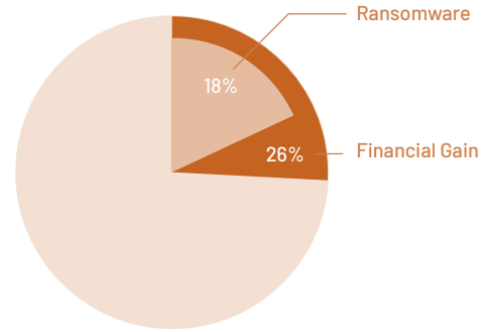
STATE OF GLOBAL INDUSTRIES CYBER-SECURITY



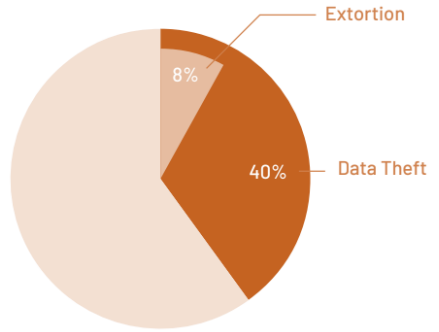
ADVERSARY ORDER OF OPERATIONS



INITIAL INFECTION VECTOR (WHEN IDENTIFIED)



ADVERSARY OPERATIONS (FINANCIAL GAIN)



ADVERSARY OPERATIONS (DATA THEFT)


INDIVIDUAL
VVIPS
NATIONAL CRITICAL
INFRASTRUCTURE
BANK
ENTERPRISE
CYBER ATTACK SURFACE


Cloud Services & Remote Access
Attackers exploit vulnerabilities in cloud services and remote access tools to compromise data integrity or steal sensitive information.
Online Banking & Financial Transactions
Cybercriminals target online banking and payment systems to steal financial information, credentials, or conduct fraudulent transactions.
Personal Devices
Attackers target personal computers, smartphones, and tablets through malware, phishing, or software vulnerabilities, aiming to steal sensitive information, access accounts, or conduct surveillance on users.
PERSONAL SECURITY ANALYSIS
Internet of Things (IoT) Devices
Insecure IoT devices are targeted by attackers to gain unauthorized access, compromise privacy, or launch DDoS attacks.
Email Accounts
Email accounts are targeted for phishing, malware distribution, & account takeover, allowing attackers to access sensitive information or launch further attacks.
Social Media
Attackers use social media platforms to steal personal data, spread misinformation, or hijack accounts through phishing, malware, or impersonation.

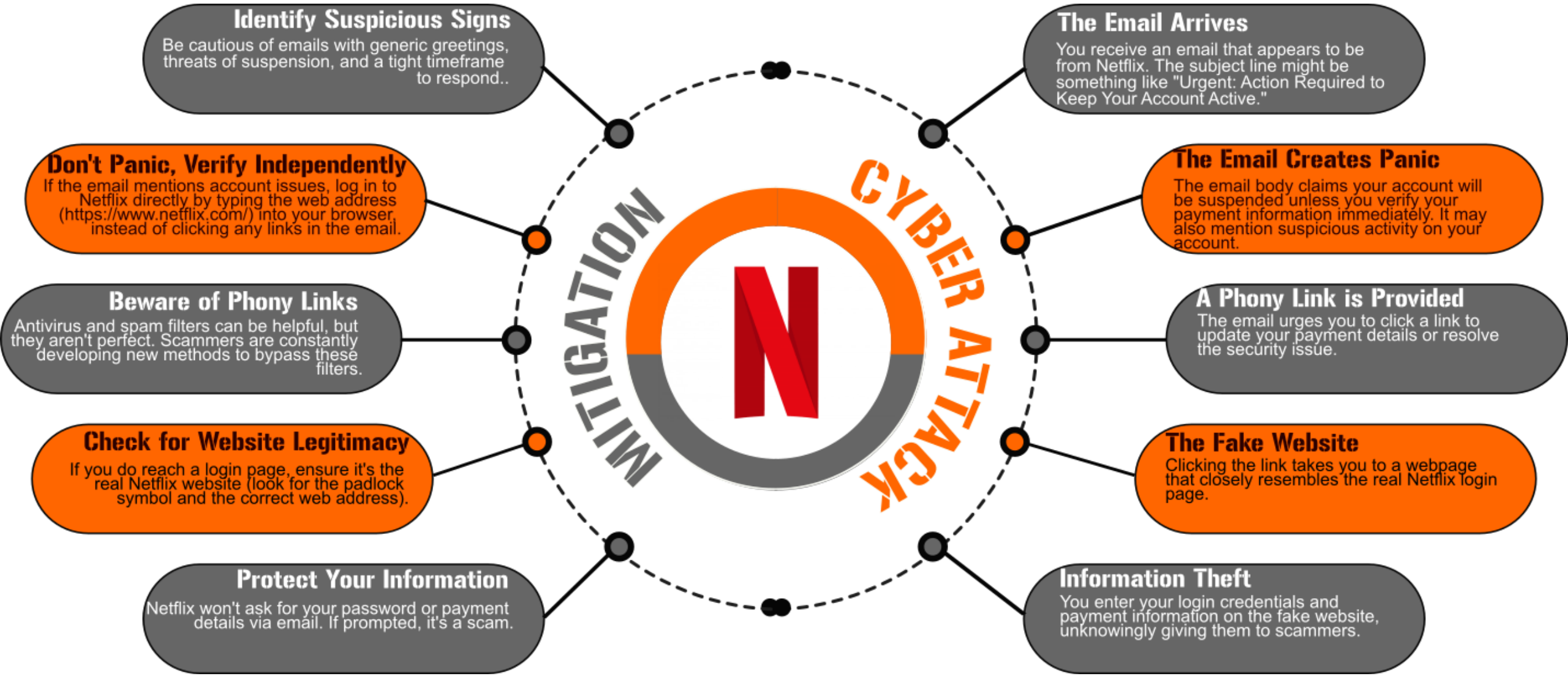
PHISHING & IDENTITY SPOOFING

NETFLIX

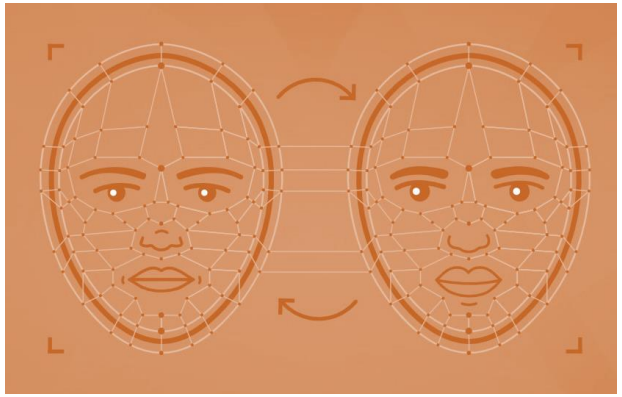
Users of the popular streaming service, Netflix, were recently targeted by a widespread phishing attack. It's estimated that days, weeks, or even years will be spent by victims attempting to restore their identity.

Approximately 100 hours of this will take place at work. On company time.

PHISHING SCENARIO



DEEPFAKE VIDEO (GENERATIVE A.I.)



An employee at a multinational firm was tricked into sending 250,000 dollars to fraudsters using deepfake video to pose as the company's CFO.

Verifying the identity of a person making a sensitive request is crucial to protecting yourself and your organization.

DEEPFAKE VIDEO ATTACK SCENARIO

Deepfake Awareness Training
Educate employees about deepfake technology and how it can be used in scams. Train them to identify suspicious elements in videos, like unnatural blinking or slight inconsistencies in speech patterns.

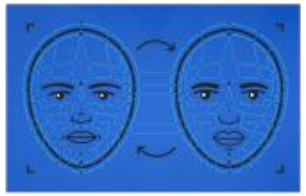
Multi-Factor Authentication
Implement multi-factor authentication (MFA) for all financial transactions and access to sensitive information. This adds an extra layer of security beyond just passwords.

Verification Protocol
Establish a clear verification protocol for any urgent or unusual requests, especially those involving large sums of money. This could involve requiring confirmation directly from the CFO (through a trusted channel).

Encourage Reporting
Foster an open environment where employees are encouraged to report suspicious emails or requests, even if they seem to come from high-level figures.

Protect Your Information
Regularly conduct cybersecurity drills to test employee preparedness and identify vulnerabilities in communication protocols.

MITIGATION



CYBER ATTACK

Deepfake Creation
Scammers create a video using deepfake tech, impersonating the CFO endorsing a scam.

The Email Creates Panic
The scammers identify high-level employees within the company with access to finances or sensitive information. Emails with the deepfake video are sent to high-level employees, posing as trusted colleagues.

Urgency and Pressure
The emails will create a sense of urgency and pressure the recipients to act quickly. They might emphasize the confidentiality of the information or the time-sensitive nature of the CFO's "instructions."

Exploiting Trust
The deepfake video, coupled with the impersonation emails, leverages trust within the organization to bypass normal verification procedures.

Financial Loss
The deceived employees follow the fraudulent instructions in the video, leading to unauthorized transfers or investments, causing significant financial losses to the company.

PUBLIC WI-FI & VPN

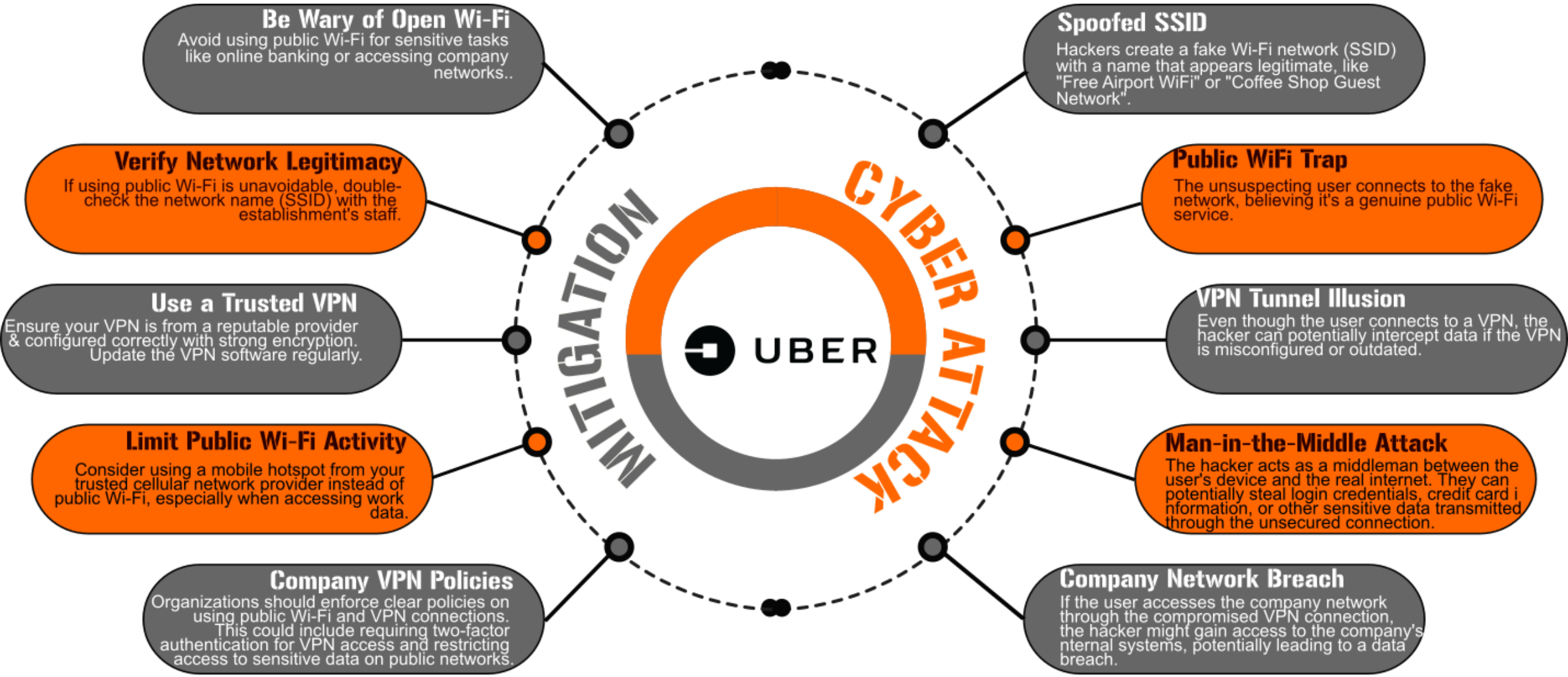
Uber

For over a year the ride-sharing service, Uber hid a hack that exposed the sensitive data of 57 million of its users and drivers.

The stolen information included names, driver's license numbers, email addresses and phone numbers.

Uber paid the hackers $100,000 to destroy the stolen data and keep the breach quiet, further eroding the public's trust.

PUBLIC WI-FI & VPN ATTACK SCENARIO

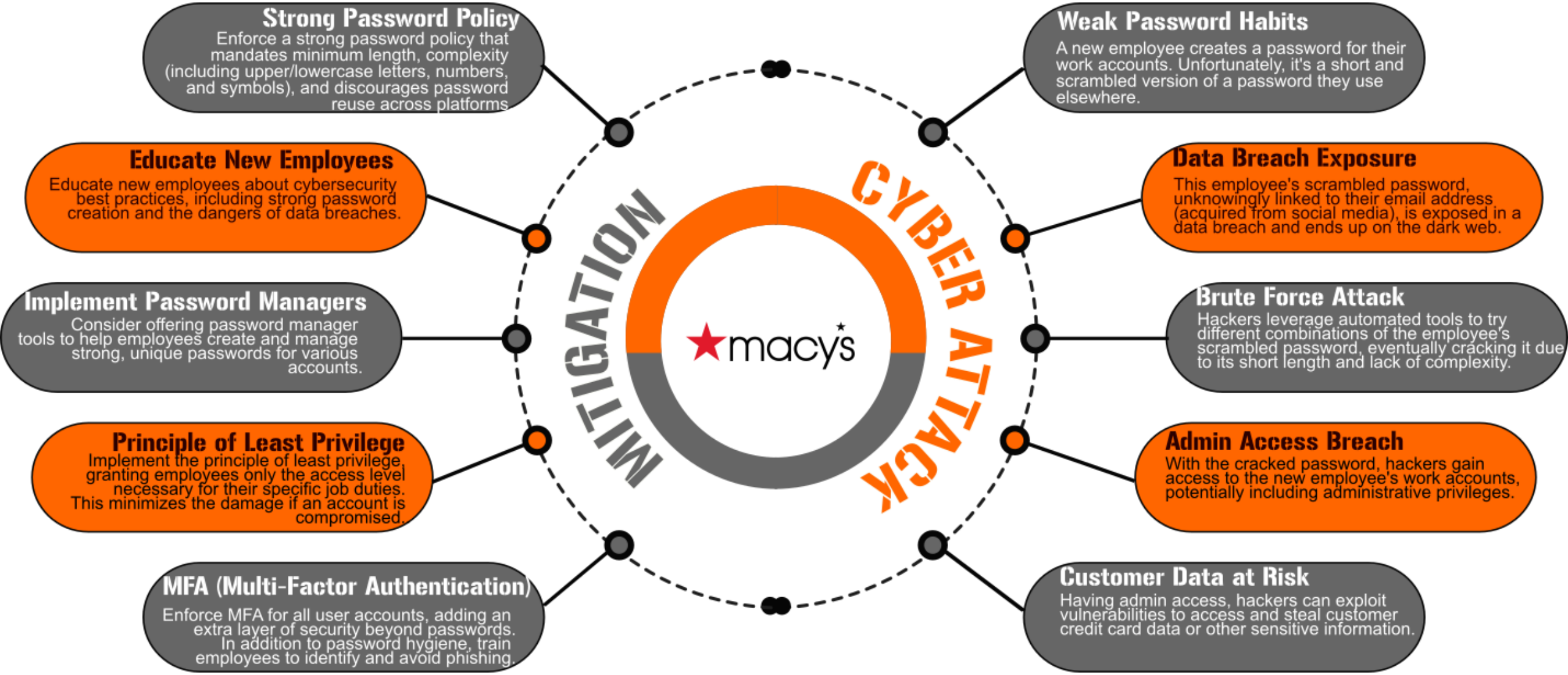


REUSED PASSWORDS

Macy's offers co-branded credit cards with American Express, but also has its own store card. Stock prices for Macy's Incorporated plummeted after the retailer disclosed that attackers installed malicious code on their website, allowing them to steal credit card information from Macy's customers.

This was the second time in two years Macy's has been hacked.

PASSWORD BREACH SCENARIO

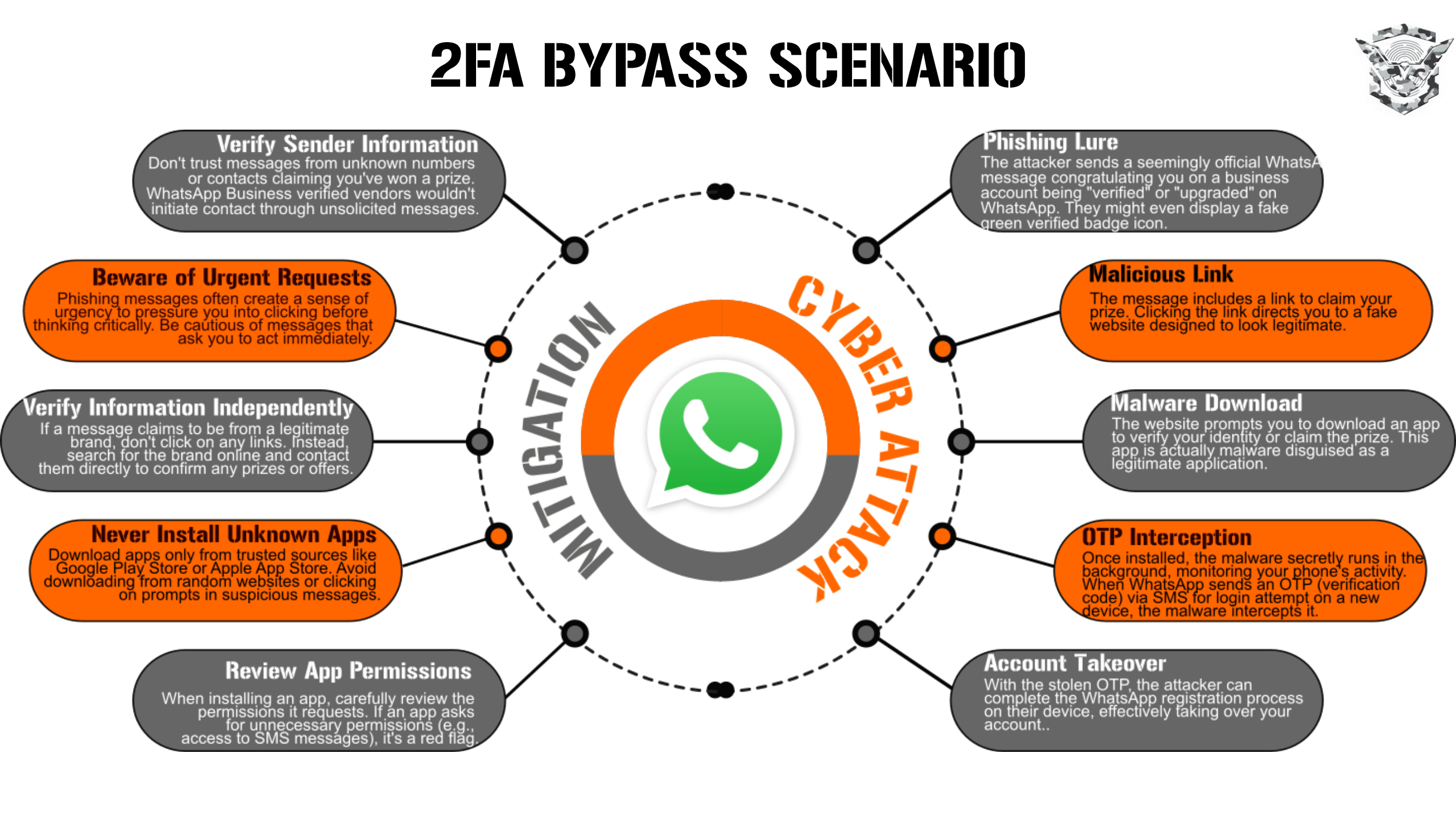


2 FACTOR AUTHENTICATION (2FA) BYPASS

Security experts are seeing a massive increase in malware OTP interceptors available online.

These malicious programs steal one-time passwords (OTPs) used for two-factor authentication (2FA). Once stolen, attackers can use the OTPs to bypass 2FA and gain access to a victim's sensitive accounts such as banking, social media, and E-commerce platforms.

2FA BYPASS SCENARIO



Verify Sender Information
Don't trust messages from unknown numbers or contacts claiming you've won a prize. WhatsApp Business verified vendors wouldn't initiate contact through unsolicited messages.

Beware of Urgent Requests
Phishing messages often create a sense of urgency to pressure you into clicking before thinking critically. Be cautious of messages that ask you to act immediately.

Verify Information Independently
If a message claims to be from a legitimate brand, don't click on any links. Instead, search for the brand online and contact them directly to confirm any prizes or offers.

Never Install Unknown Apps
Download apps only from trusted sources like Google Play Store or Apple App Store. Avoid downloading from random websites or clicking on prompts in suspicious messages.

Review App Permissions
When installing an app, carefully review the permissions it requests. If an app asks for unnecessary permissions (e.g., access to SMS messages), it's a red flag.

Phishing Lure
The attacker sends a seemingly official WhatsA message congratulating you on a business account being "verified" or "upgraded" on WhatsApp. They might even display a fake green verified badge icon.

Malicious Link
The message includes a link to claim your prize. Clicking the link directs you to a fake website designed to look legitimate.

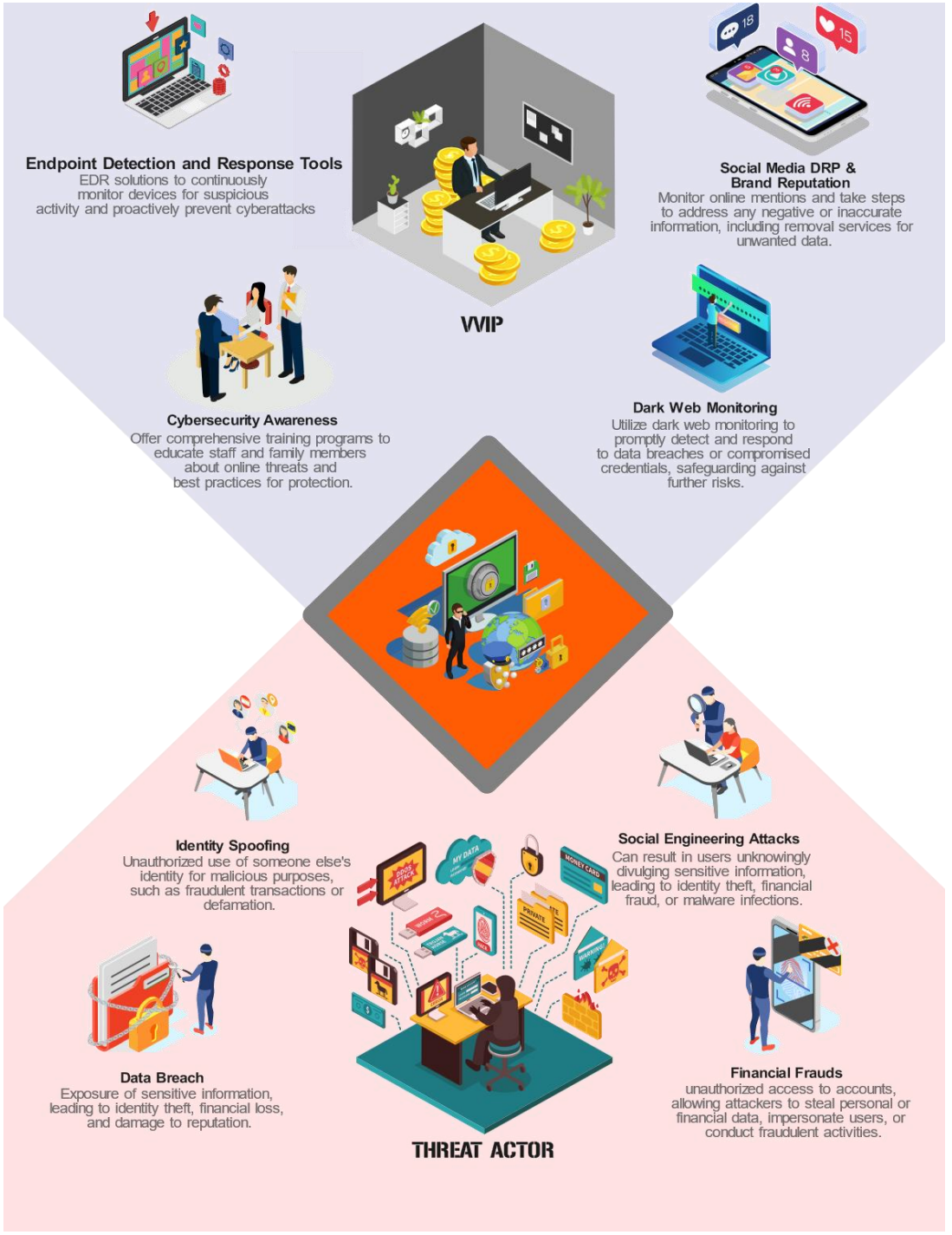
Malware Download
The website prompts you to download an app to verify your identity or claim the prize. This app is actually malware disguised as a legitimate application.

OTP Interception
Once installed, the malware secretly runs in the background, monitoring your phone's activity. When WhatsApp sends an OTP (verification code) via SMS for login attempt on a new device, the malware intercepts it.

Account Takeover
With the stolen OTP, the attacker can complete the WhatsApp registration process on their device, effectively taking over your account..

VVIP CYBERSECURITY

VVIP THREAT ATTACK SURFACE



NOTABLE CYBER ATTACKS ON VVIPs

DNC Email Hack (2016): Russian hackers breached DNC systems, leaking internal emails to influence the 2016 US election, highlighting the need for strong cybersecurity in political organizations.

Jeff Bezos Phone Hack (2018): Jeff Bezos' phone was reportedly hacked via a malicious WhatsApp video, showcasing the dangers of social engineering attacks and the importance of cautious messaging.

iCloud

iCloud Photo Leak (2014): Celebrities' iCloud accounts were breached, exposing private photos due to weak authentication. This underscores the need for robust passwords and multi-factor authentication.

Monaco Money Laundering Ring (2016): Cybercriminals targeted a European bank, infiltrating systems via phishing. They siphoned €1 billion, illustrating the risk of social engineering and the need for heightened cybersecurity in financial institutions.

SERVICES FOR VVIPs

				
Dedicated Account Management: VVIPs typically get assigned a dedicated security and medical account manager. This personal point of contact ensures all their needs are addressed promptly and they have a trusted advisor for any situation.	**Enhanced Evacuation and Repatriation:** In case of emergencies or critical situations, Fourth Command prioritizes VVIPs evacuation and repatriation. This can involve arranging secure transportation, medical assistance during transit, and ensuring a smooth return home.	**Increased Response Times:** High Priority Individuals benefit from faster response times for any assistance they require. This could be anything from medical consultations to security advice, ensuring their concerns are addressed with the utmost urgency.	**Bespoke Threat and Risk Assessments:** Fourth Command goes beyond general briefings for VVIPs. We offer customized threat and risk assessments based on the individual's travel itinerary, profile, and potential vulnerabilities. This allows for proactive security measures and mitigation strategies.	**24/7 Global Assistance with Discretion:** Executives can expect uninterrupted support from International SOS, 24 hours a day, 7 days a week, anywhere in the world. We understand the need for confidentiality and ensures discretion in handling all HPI requests.

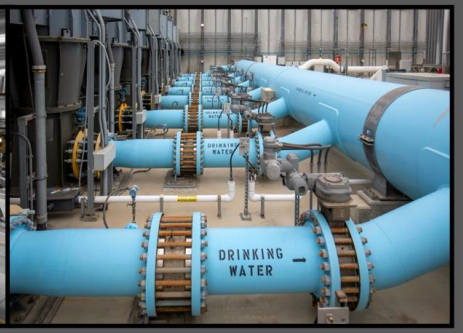
Chemical Plant

Pharmaceutical

Power Plant

Transportation

Manufacturing



De-salination Plant

BMS (Building Management System)

Oil and Gas

Water Treatment Plant

ENTERPRISE CYBER DEFENSE

INDUSTRY DRIVEN BY COMPLIANCE

REGIONAL CYBERSECURITY REGULATORY FRAMEWORKS

هيئة أبوظبي الرقمية
ABU DHABI DIGITAL AUTHORITY

DUBAI ELECTRONIC SECURITY CENTER
مركز دبي للأمن الإلكتروني

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الهيئة الوطنية للأمن الإلكتروني
NATIONAL ELECTRONIC SECURITY AUTHORITY
UNITED ARAB EMIRATES الإمارات العربية المتحدة

FINANCE

- Banks, Insurance Providers, Payment Gateways
- Regional Cybersecurity Frameworks

- International Frameworks

HEALTHCARE

- Hospitals, Health Authority, Health Insurance Provider
- Regional Cybersecurity Frameworks


- International Frameworks

NOTABLE CYBER ATTACKS

Stuxnet (2010): One of the most infamous cyber attacks targeted the Iranian nuclear program but also affected industrial control systems, including those used in manufacturing plants. Stuxnet specifically targeted programmable logic controllers (PLCs) used in supervisory control and data acquisition (SCADA) systems.

NotPetya (2017): Although it initially targeted Ukrainian infrastructure, the NotPetya ransomware spread globally, affecting numerous organizations including manufacturing plants. NotPetya encrypted hard drives, rendering systems inoperable and causing significant disruption to operations.

Trisis/Triton (2017): This malware targeted safety instrumented systems (SIS) in industrial control systems, aiming to cause physical damage to manufacturing facilities. Trisis/Triton's discovery raised concerns about the vulnerability of critical infrastructure to cyber attacks.

LockBit (2020): LockBit is a type of ransomware that has targeted manufacturing companies, encrypting their systems and demanding payment for decryption keys. These attacks can halt production, leading to significant financial losses.

APT33 (2019): This Iranian state-sponsored hacking group has targeted aerospace, energy, and manufacturing sectors. APT33 has used tactics such as spear-phishing and malware to gain access to critical systems.

Infusion Pumps

Medical Workstations

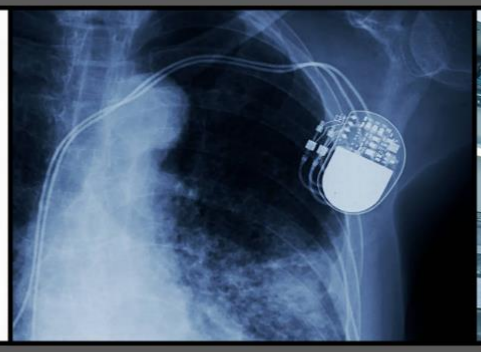
Medical Imaging

Patient Monitoring System

Wearables

Smart Beds

Insulin Pumps



Pacemaker

Pneumatic Tubes System

POST COVID ERA

HEALTHCARE | IoMT CYBER DEFENSE

CYBER ATTACKS ON HEALTHCARE

Anthem Inc. (2015): This cyberattack exposed the personal information of over 78 million people, including patients, employees, and dependents. Hackers gained access through a sophisticated attack and stole a vast amount of data.

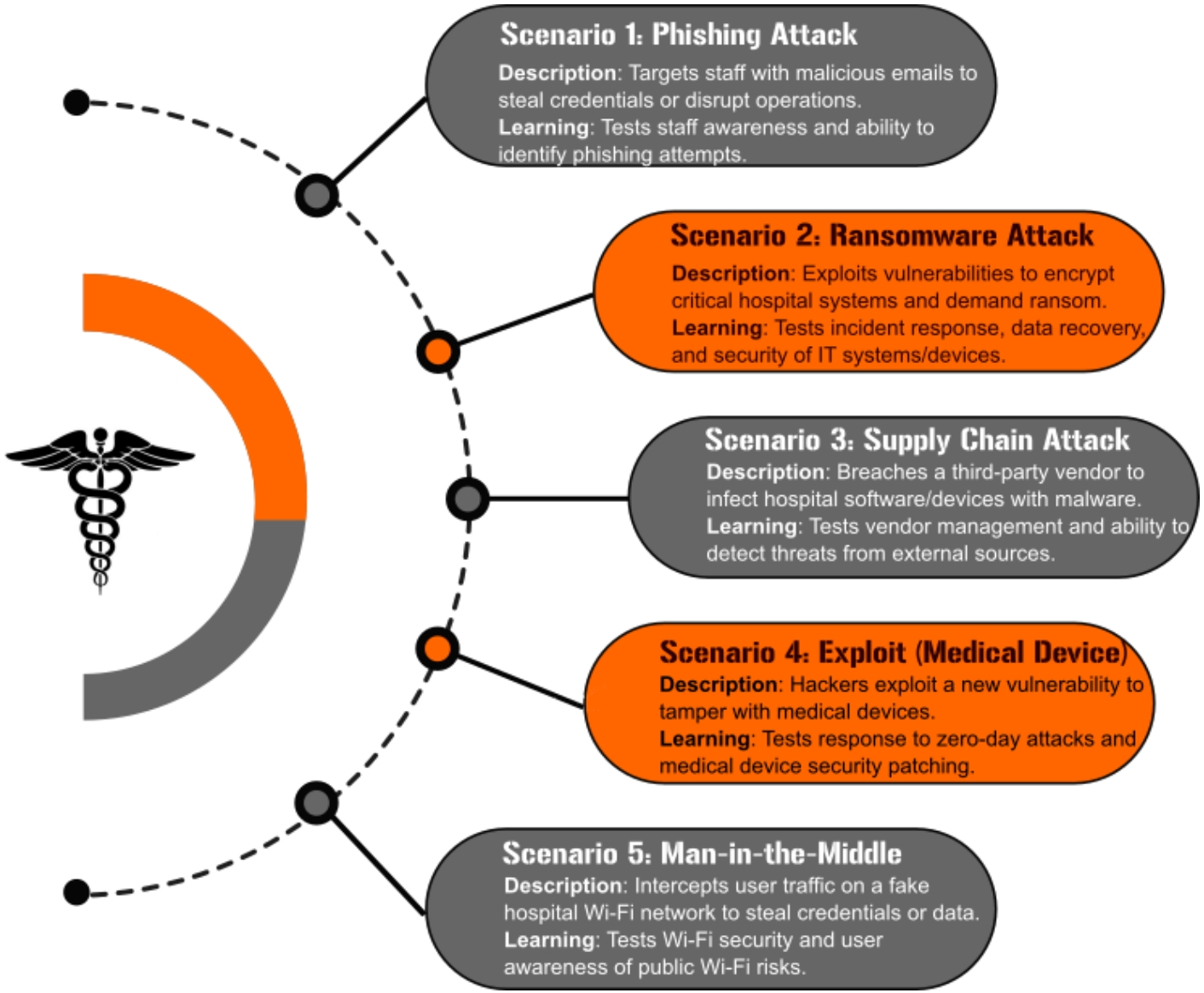
HACKED

Medibank Private (2023): This Australian health insurer was targeted in a ransomware attack. Hackers stole personal information from millions of customers, including health records. The attack caused significant disruption and raised concerns about the security of patient data in Australia.

Trin beratu third- trans nity H xpose near incid owca associated with relying on external vendors and the importance of robust data security practices throughout the entire healthcare ecosystem.

Banner Health (2016): Hackers infiltrated Banner Health's network through a seemingly innocuous entry point - their food and beverage outlet's payment processing system. This highlights how attackers can exploit seemingly unrelated systems to gain access to sensitive information.

HEALTHCARE: CYBER ATTACK SCENARIO



In our interconnected world, cyber warfare threatens our very foundation. But there's hope. By embracing cyber awareness and responsibility, we can create a thriving, secure digital economy. Let's unite to deter threats, support law enforcement, and safeguard our online world.

STAY CYBER SAFE!