

The Human Factor in Cyber Operations

From cybercriminal campaigns to online foreign influence and cyber terrorist operations, how threat actors exploit human vulnerabilities to achieve their goals?

By Jeremy Makowski
CyberCrime and Terrorism Intelligence Expert

February 2024

Table of Contents

1. Executive Summary 2

2. Understanding Human Behaviour in Cyberspace 3

3. Techniques and Modus Operandi 7

    3.1 Social Engineering 7

    3.2 Artificial Intelligence and Machine Learning 15

    3.3 Virtual HUMINT 18

4. The Human Factor in Cybercrime Operations 22

5. The Human Factor in Cyberwarfare and Influence Operations 23

6. The Human Factor in Cyber Terrorism Operations 27

7. Conclusion 29

8. About The Author 30

1. Executive Summary

For almost twenty years, technologies have continued to evolve and become part of our daily lives. From social networks to smartphones and other Internet-connected objects, including all kinds of applications, cyberspace has become a parallel world with more and more impact on our physical world. Even though humans have adapted relatively well to this new digital world and have learned to use new technologies, they remain very vulnerable to threat actors. If a system has some vulnerabilities, the biggest is human. Although man evolves, he remains, as his name suggests, a man with these strengths and, above all, these weaknesses. If computer systems can be hacked and abused, so can humans. Over time, thanks to social engineering, virtual HUMINT, and artificial intelligence, threats have learned to exploit human weaknesses and play on human aspects such as fear, curiosity, excitement, sexual attraction, guilt, anger, and sadness to achieve their illicit goals.

From cybercriminal phishing or ransomware campaigns to those of state-linked and terrorist groups on disinformation and influence, the human factor is undoubtedly the critical element in the success of a cyber operation. This document aims to review, analyze, and explain the different mechanisms threat actors use during their cyber operations. The investment by governments and private companies of billions of dollars in systems to protect and prevent cyber operations can often seem excessive when we know that most threat actors succeed in circumventing all of these systems by exploiting human credulity. The prevention of these malicious cyber operations must first and foremost involve good people training. Getting informed, checking, comparing, and questioning are the essential elements in the prevention chain.

2. Understanding Human Behaviour in Cyberspace

For several years, the development and expansion of cyberspace have given rise to a new digital way of life. The almost total digitalization of all goods and services has forced humans to adapt to this way of life. In January 2024, the Kepios company published a report that provided a certain amount of data concerning the relationship between the world population and the number of people connecting to the internet using smartphones or social networks (Figures 1 and 2).[1] We can observe that most of the world's population is directly or indirectly connected with digital life.

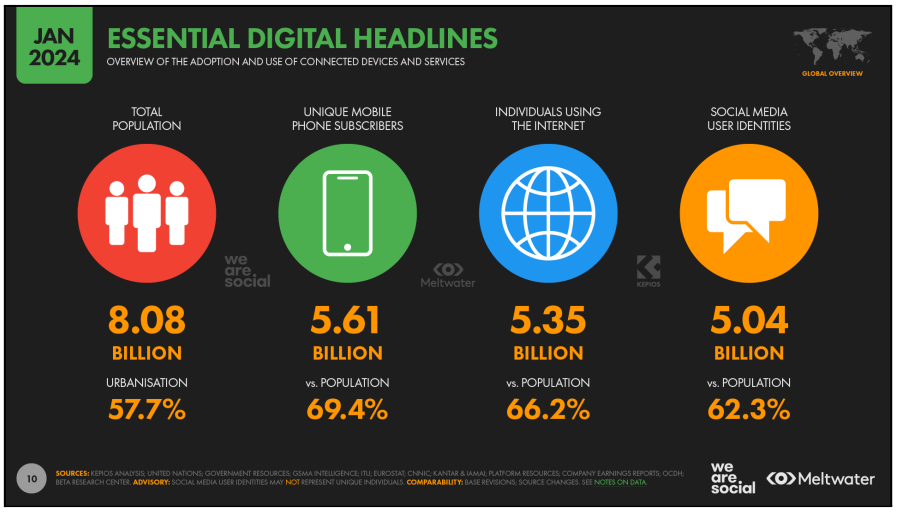


Figure 1 - Global essential digital headlines in 2024 (Source: Kepios)

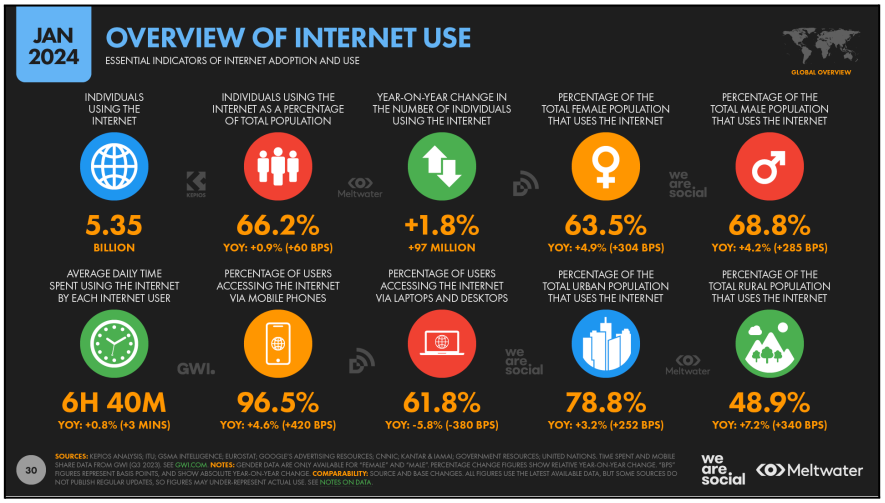


Figure 2 - Global overview of Internet use in 2024 (Source: Kepios)

[1] *https://datareportal.com/reports/digital-2024-global-overview-report*

In addition, Kepios shows the reasons and types of Internet use (Figures 3 and 4).

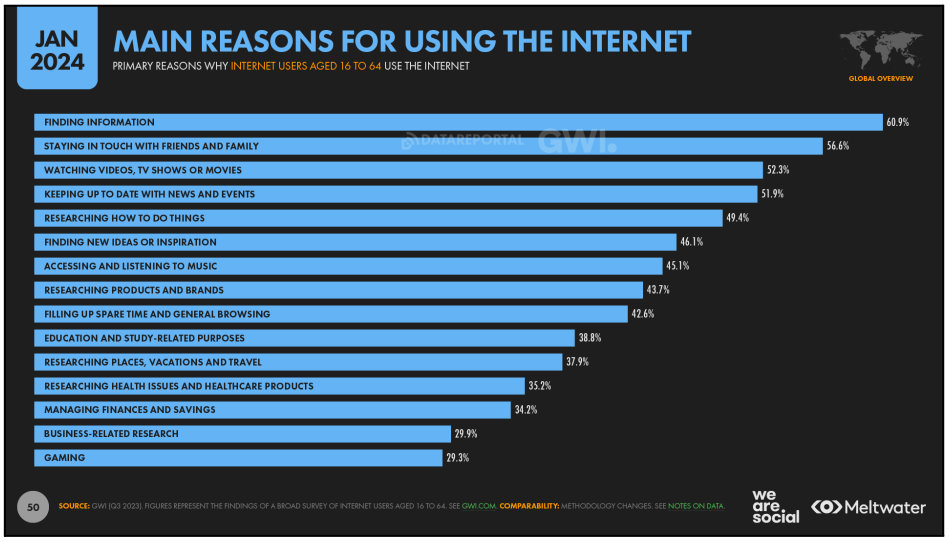


Figure 3 - Global main reasons for using the Internet in 2024 (Source: Kepios)

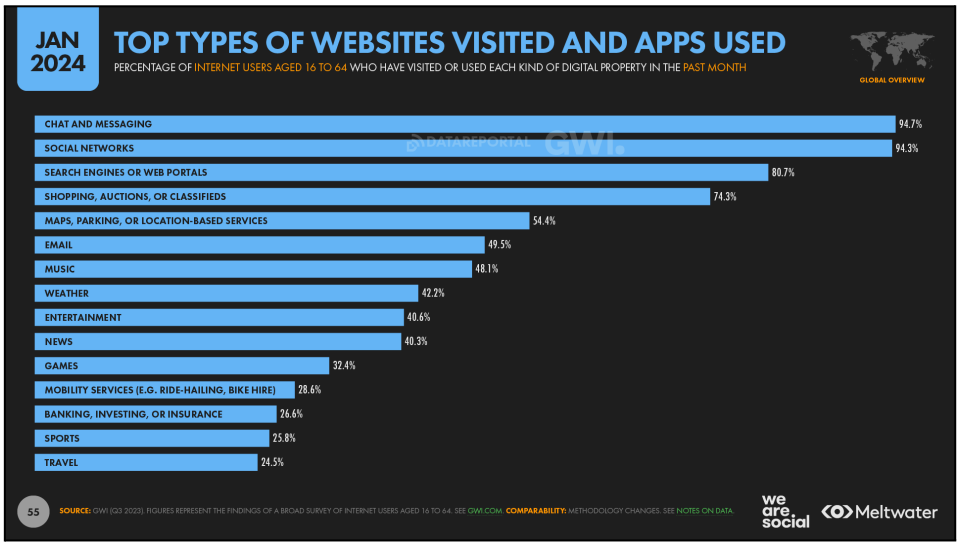


Figure 4 - Global top types of websites and applications used (Source: Kepios)

Human-machine interaction (computers, smartphones, tablets, cameras, vending machines, cash registers, etc.) is now ubiquitous, resulting in very different human-to-human interactions. The development of social networks and applications has fundamentally changed human behavior. Indeed, this expansion of cyberspace and the sharp increase in accessible information and data significantly impact humans. It is often difficult for humans to absorb a large quantity of data daily but extract and understand the most important without getting lost and confused in this mass. The spread of fake sites, news, and data only makes this interaction between man and machine more difficult.

In 2018, a study was conducted by three MIT researchers revealing that fake news spreads faster on the social network X (formerly Twitter) than real news, and by a considerable proportion.[2] Since then, universities worldwide have conducted other studies, such as the American USC, explaining that the biggest influencing factor in the spread of fake news likely lies in the structure of social platforms that reward users for habitually sharing information. According to USC researchers, misinformation spreads because users lack the critical thinking skills to discern truth from lies or because their solid political beliefs distort their judgment.[3]

If artificial intelligence is increasingly present, it facilitates and improves certain things; it is also a source of risks regarding its fraudulent use. AI enables the generation of information propagated en masse without being verified or false, provoking opinion movements, or manipulating and deceiving populations. In addition, thanks to AI, it is now very easy to impersonate a person's visual and vocal identity and make them say anything.

In addition to a lack of verification and questioning of the data received, humans want to go even faster when operating in cyberspace. Excessive consumption of websites, applications, images, and videos often reduces vigilance when visiting a critical site such as a bank or government. Suppose many public and private institutions have implemented Multi-Factor Authentication principles. In that case, many people worldwide find themselves deceived and misled due to a lack of vigilance and a desire to go even faster when searching to connect to a site that could be considered sensitive. Cyber security experts from many countries have understood for several years now that humans are, without a doubt, the biggest vulnerability (Figure 5).

[2] https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308
[3] https://today.usc.edu/usc-study-reveals-the-key-reason-why-fake-news-spreads-on-social-media/

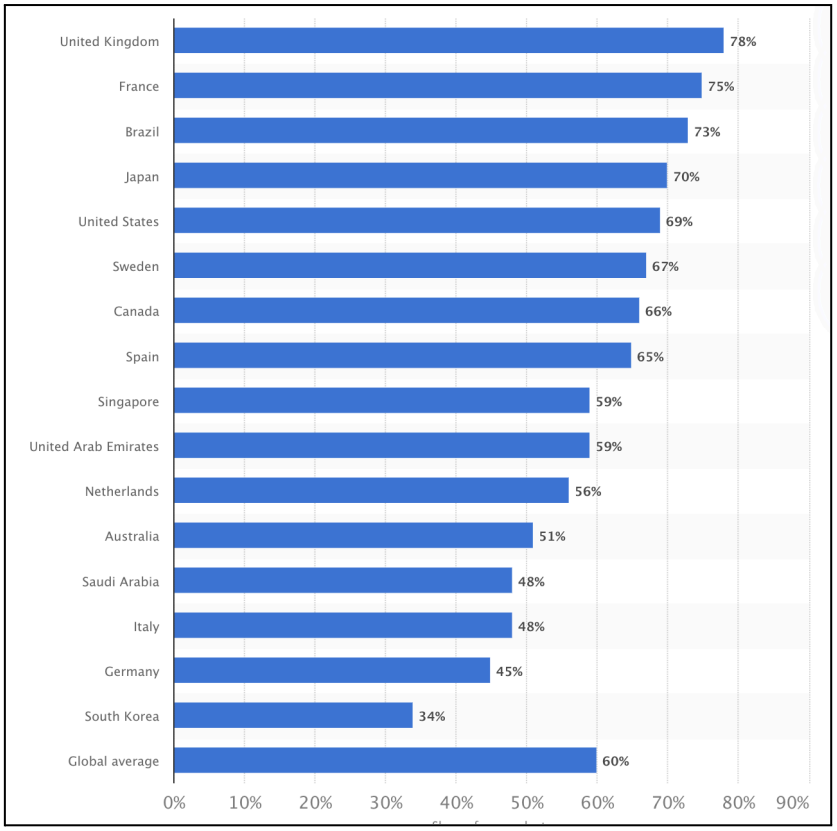


Figure 5 - Percentage of CISOs assessing that human error is their organization's biggest cyber vulnerability globally in 2023 by country (source: Statista)

However, a significant lack of knowledge and information about the risks and threats in cyberspace among private and public sector employees and the general public allows many threat actors to manipulate them into carrying out fraudulent operations or encourage them to make mistakes and thus achieve their ends. Cybersecurity company Proofpoint says more than 90% of cyberattacks require user interaction.[4] Simple user actions, like mistaken clicks and misused passwords, can have serious consequences. This human factor is also present when we talk about the security of computer networks and systems. Suppose we can bypass the security of a machine or system. In reality, this is only possible because humans lack vigilance or a certain vision of security when designing it, even if a system is secure. does not exist and will never exist.

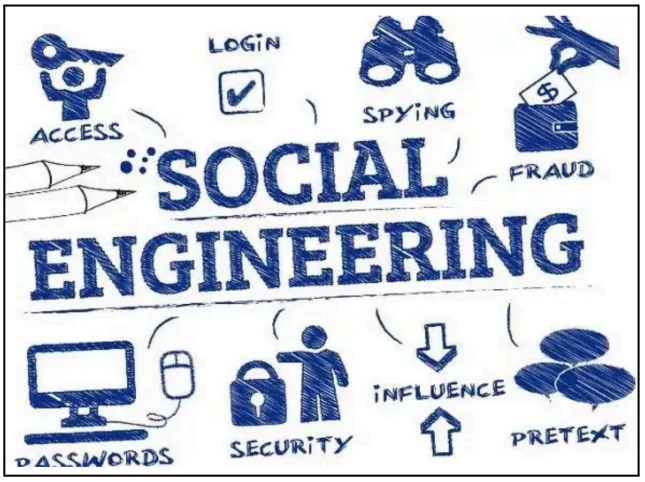
[4] https://www.proofpoint.com/us/blog/email-and-cloud-threats/how-human-behavior-impacts-cybersecurity

3. Techniques and Modus Operandi

To exploit human weakness and achieve their goals, threat actors use various techniques and operating methods, allowing them to approach, manipulate, and deceive their targets. These techniques are robust attack vectors that are known and famous.

3.1 Social Engineering

Social engineering is one of threat actors' most well-known techniques to exploit human vulnerabilities. It refers to a wide range of malicious activities carried out through human interactions, including using psychological manipulation to trick users into making security errors or disclosing sensitive information. Social engineering attacks usually involve the following stages:



Collection: This first step typically involves collecting strategic and technical information about the target, such as key people, potential entry points, and security weaknesses.

Approach: This first step involves establishing a voice or written contact with the victim and building a trusted relationship.

Manipulation: This step is the logical continuation of the previous one. Once the trusted relationship has been established and the victim's weaknesses detected, the threat actor can psychologically manipulate his victim to obtain from him what he wishes to obtain.

Disengagement: This last step implies that once the threat actor has obtained the information or actions carried out by the victim in his favor, he stops being in touch with the victim in the most natural way possible, depending on the context and the cover story created.

Psychological manipulation is the key to social engineering success. To carry out their attacks, the most experienced threat actors often study human behavior in cyberspace. They exploit human weaknesses by relying, among other things, on the victims' lack of confidence and their poor or weak knowledge of the cyber environment. Indeed, in the same way that some people feel vulnerable on board a plane because they do not control the environment, the same phenomenon can be observed in cyberspace. Cyberspace is a vast ocean of devices, connections, systems, applications, and actors that is difficult for many people to understand and control. Suppose that humans have more or less succeeded in getting used to cyberspace and its codes (websites, applications, QR codes, 2FA, cookies, etc…); nonetheless, they need to be better informed of the risks and threats incurred. This phenomenon is even more marked among seniors who have not been able to adapt to this new world. Psychological manipulation of the victim can be carried out based on the following principles.

Emotions: emotional manipulation generally gives a strategic advantage to the threat actor when interacting with his victim. The victim is much more likely to take irrational or risky actions without realizing it when in a heightened emotional state. Threat actors generally use the following emotions to convince their victims: fear, curiosity, excitement, guilt, anger, and sadness.

Emergency: Urgent situations or requests are another reliable tool in a threat actor’s arsenal. A victim can compromise themselves under the cover of a serious problem that requires immediate action.

Confidence: Confidence and credibility are essential during a social engineering attack. The threat actor generally does in-depth research on his victim, allowing him to create a story that is easy to believe and unlikely to arouse suspicion.

Besides these types of manipulation, threat actors can also use more direct methods to access a network or an organization's computer, such as frequenting the public restaurant or rest area of a large office building, replacing the free wifi network by impersonating it to create a honeypot to collect information about users.

Email and SMS phishing are threat actors' most popular and effective social engineering techniques. The creators of phishing campaigns generally seek to play on factors of importance, urgency, security, curiosity, or fear among victims. Threat actors pose as trusted institutions or individuals to trick their victims into revealing sensitive information, clicking links to malicious websites, or opening attachments containing malware. To lend credibility to their actions, many threat actors include false secure connection signals to trick the victim into believing that the site they enter their data into is secure (Figure 6).

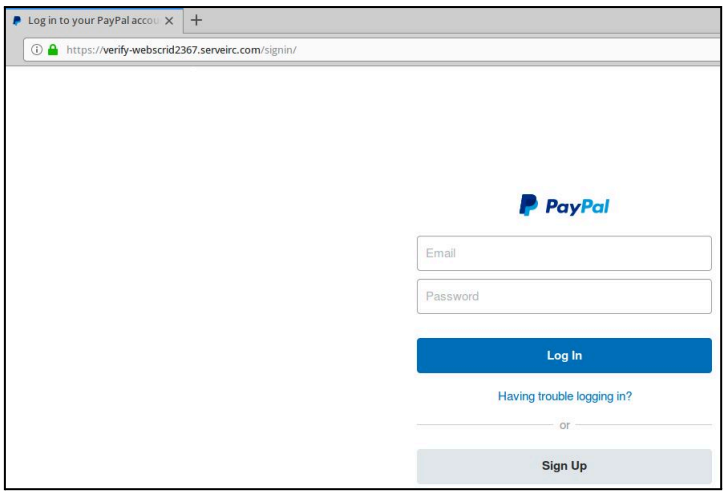


Figure 6 - A phishing page that uses https:// and has the green padlock.

There are several types of phishing attacks, but the most popular are the following:

Email phishing is the most traditional means of phishing, using an email urging you to reply or follow up by other means. Web links, phone numbers, or malware attachments can be used (Figure 7). This type of campaign can target a specific category of people (customers of a company or subscribers to a service) or a wider audience with a certain percentage of success on large volumes of email sending.

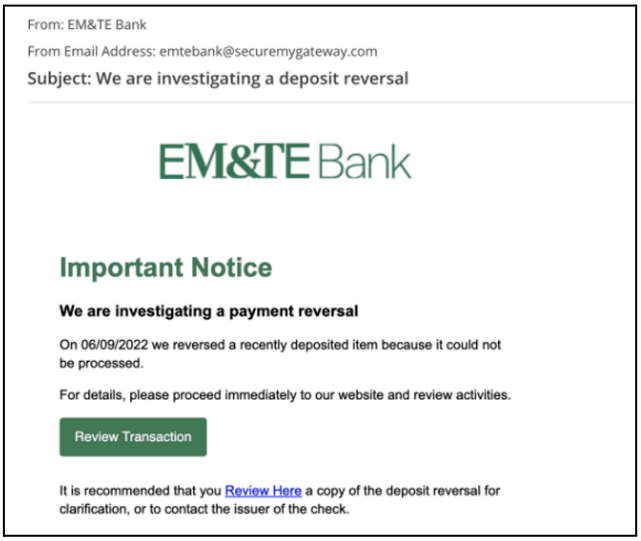


Figure 7 - Bank account verification phishing email example (Source: Keepnet Labs)

SMS phishing (Smishing) is done via text or instant messaging. Typically, threat actors distribute links to redirect to a malicious website or download malicious software stealthily. The emergence of smishing as a tactic results directly from employees using smartphones to access both their text messages and corporate emails (Figure 8). As with email phishing, threat actors generally obtain lists of telephone numbers from hacked customer databases to target a category of person.

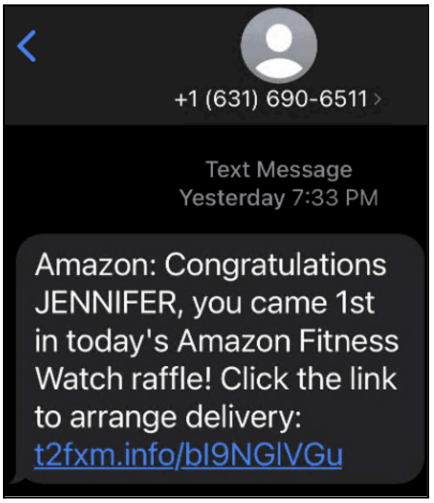
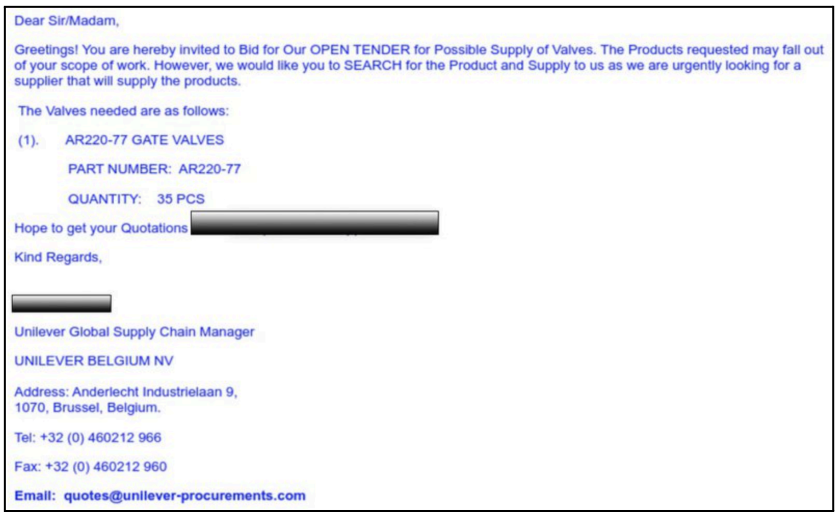


Figure 8 - Amazon SMS phishing example (Source: SafetyDetectives)

Business email compromise (BEC) is one of the most financially damaging online social engineering techniques. It exploits the fact that everyone relies on email to conduct their activities, both personal and professional. In a BEC scam, scammers typically send an email from someone within an organization by spoofing their email address and sending what may be considered a legitimate request addressed to a victim within the same organization or being a customer, supplier, or financial partner (Figure 9).


Dear Sir/Madam,

Greetings! You are hereby invited to Bid for Our OPEN TENDER for Possible Supply of Valves. The Products requested may fall out of your scope of work. However, we would like you to SEARCH for the Product and Supply to us as we are urgently looking for a supplier that will supply the products.

The Valves needed are as follows:

(1). AR220-77 GATE VALVES

PART NUMBER: AR220-77

QUANTITY: 35 PCS

Hope to get your Quotations [redacted]

Kind Regards,

[redacted]

Unilever Global Supply Chain Manager

UNILEVER BELGIUM NV

Address: Anderlecht Industrielaan 9,
1070, Brussel, Belgium.

Tel: +32 (0) 460212 966

Fax: +32 (0) 460212 960

Email: quotes@unilever-procurements.com

Figure 9 - A BEC email targeting a multinational manufacturing organization with email impersonation from a third-party vendor. (Source: Fortra PhishLabs)

Quishing (QR code phishing) is a technique where hackers embed malicious links or files in QR codes to evade detection. The threat can bypass email filters that lack QR code detection or reading capabilities. Unlike emails containing a visible link or attachment, it can also make it more challenging for users to diagnose a threat (Figure 10).

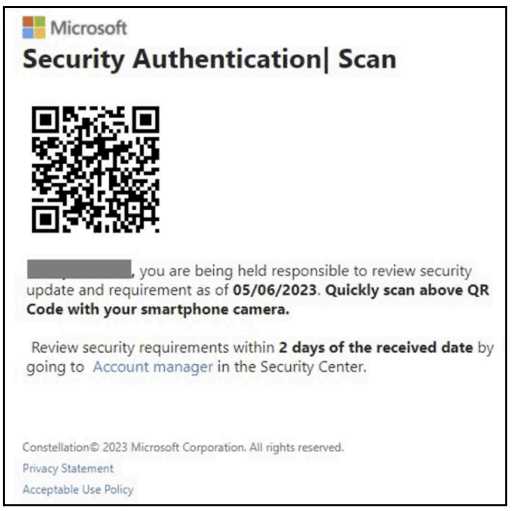


Figure 10 - Microsoft 365 Quishing email example (Source: Vade)

Voice phishing (Vishing) plays on human weakness and psychological manipulation. While classic phishing or smishing can be identified through careful review of the inbound message, threat actors use vishing because of the difficulty of the challenge it poses to the victim to discern the legitimacy of the caller. Vishing specialists often pose as people from customer support, IT, or financial services. They then seek to contact target people and try to extort them. This technique requires a certain amount of self-confidence on the part of the threatening actor because, at some point, he is supposed to be in vocal contact with the victim (Figure 11).

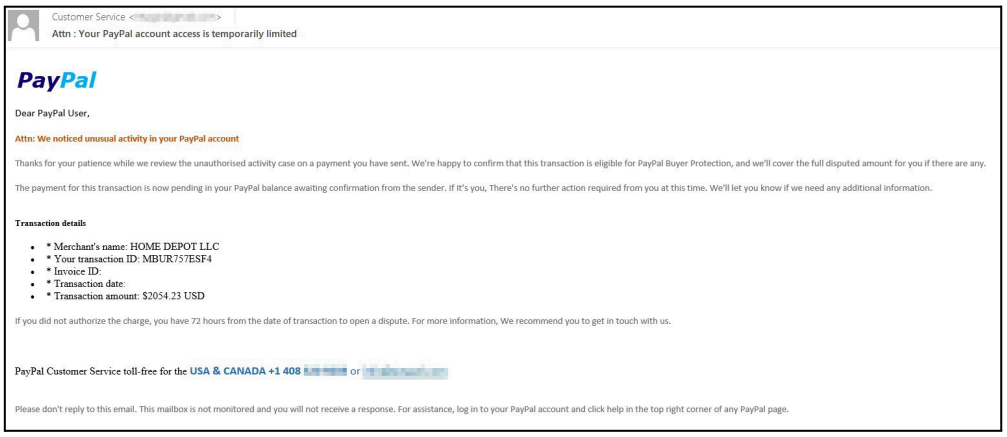


Figure 11 - Fake PayPal notification regarding order cancellation with emergency contact support

Many threat actors offer services or seek to recruit Vishing specialists on cybercriminal platforms (Figures 12 and 13).



Figure 12 - A threat actor looking to hire social engineer specialists for calls on a cybercrime forum.



Figure 13 - Professional social engineering service on a cybercrime forum

Pretexting is a social engineering attack in which a scammer invents a pretext or fabricated scenario, usually posing as a person from a public institution such as a tax authority, to trick a victim into providing sensitive personal or financial information. , such as their social security number. In this type of attack, a threat actor can also physically access your data by posing as a supplier, delivery person, or contractor to gain the trust of your staff (Figure 14).

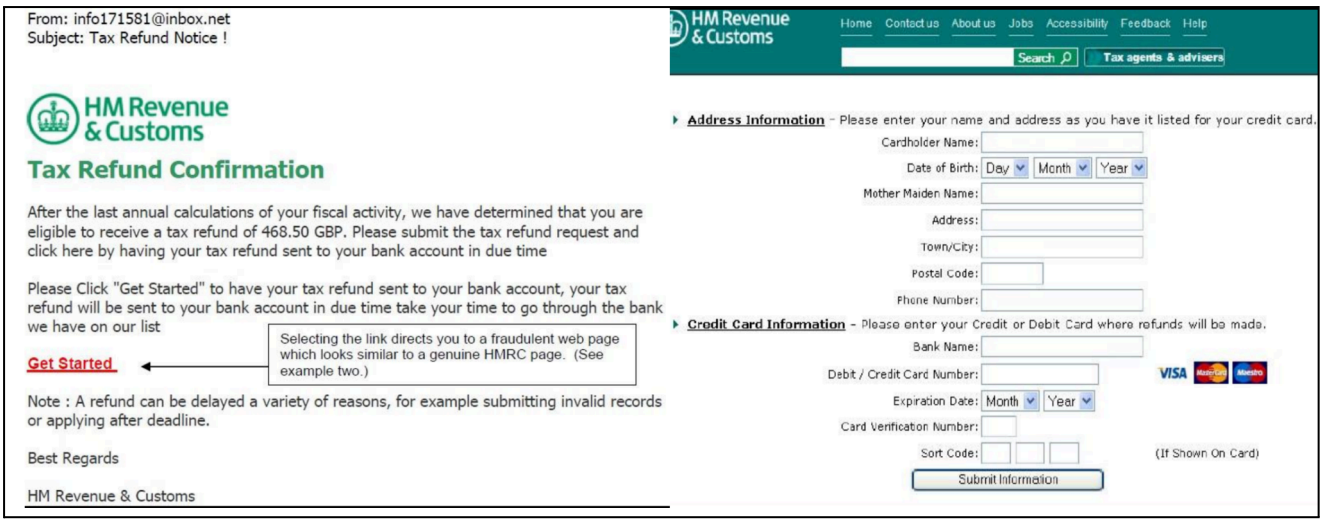


Figure 14 - Fake UK Revenue and Customs phishing pages to collect financial data

Spear phishing uses personalized information to target particular users. This information is collected through different means (leaked databases, open source, etc.). The attacks target high-value targets such as celebrities, senior executives, and high-ranking government officials. They generally pose as a known institution, a person from the same company, or the same public entity to make themselves credible (Figure 15).

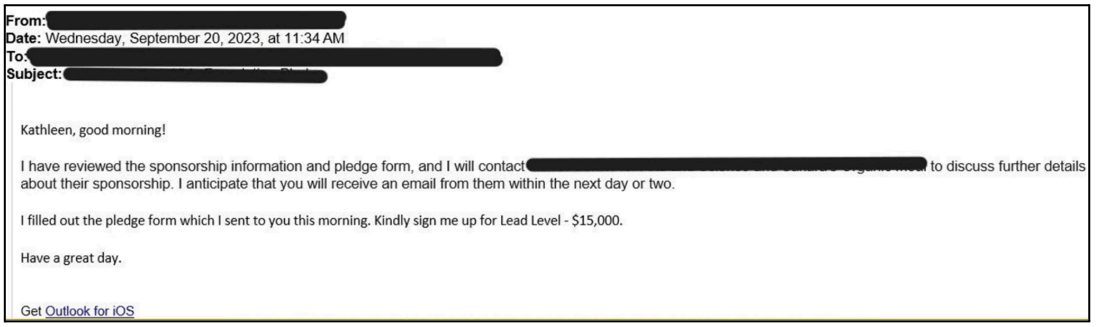


Figure 15 - Spear Email phishing example (Source: Vade)

Angler phishing is performed on social media, where an attacker imitates a trusted company's customer service team. They intercept your communications with a brand to hijack and divert your conversation into private messages, where they then advance the attack (Figure 16).

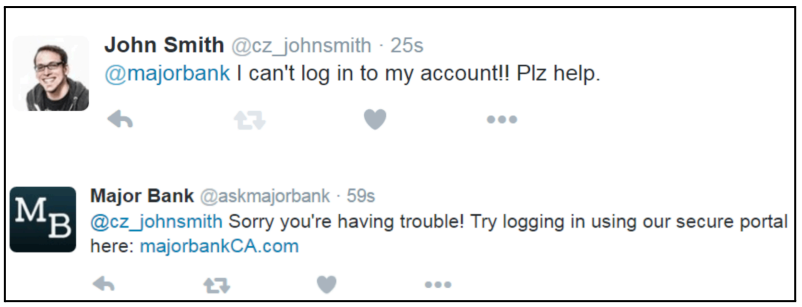


Figure 16 - Angler phishing example on X social network (Source: Proofpoint)

Search engine phishing involves indexing links to fake websites at the top of search results. These may be paid ads or legitimate optimization methods for manipulating search rankings (Figure 17).

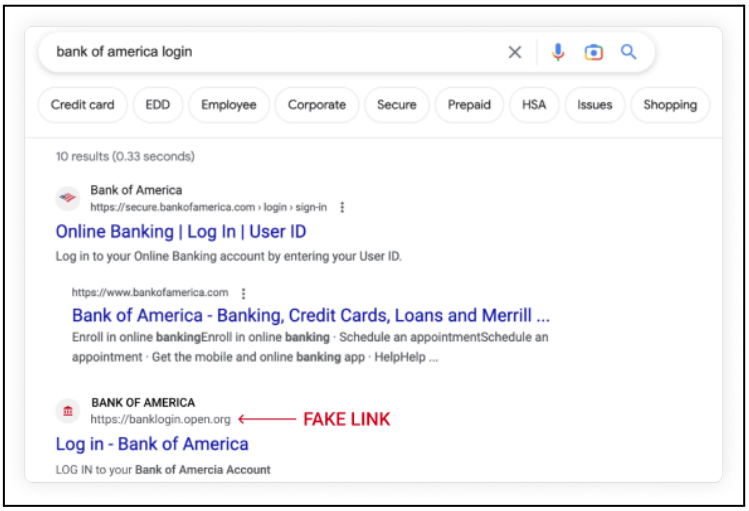
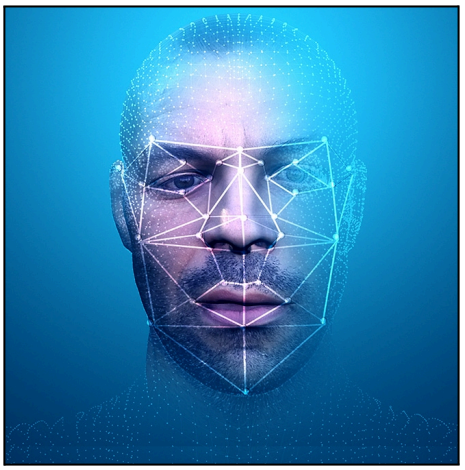


Figure 17 - Search engine phishing example (Source: Keeper)

In-session phishing interrupts everyday web browsing with fake login pop-ups for pages you're visiting.

The baiting attack involves exploiting victims' curiosity to trick them into exposing their data. Typically, threat actors lure and manipulate their victims with the help of tempting advertisements and free offers. The attack usually involves infecting the victim with malware. One of the most popular hacking methods is attaching email attachments containing details about a free offer or fraudulent freeware. Another popular form of baiting is using physical media to spread malware. Some threat actors use USB drives to infect them with malware, often leaving them statically in areas where potential victims are sure to see them and are lured by curiosity to see what the connector contains to a personal or professional computer.

3.2 Artificial Intelligence and Machine Learning



Artificial intelligence has been the subject of all fantasies for several years, and the question is, can it imitate or even replace man? Although many researchers worldwide have been working on this question for many years, it is only recently that artificial intelligence has exploded in popularity. If just ten years ago, AI was reserved for a particular industry or was mainly used in research laboratories, it is present today in many activity sectors. If AI is a significant technological advance that can help and facilitate human work, it also allows, like all technology, to be used for illicit purposes. Since the democratization of generative AI with Chat GPT by the company OpenAI, many other companies have developed AI-based tools, allowing them to create avatars and clone people's voices and faces (Figures 18 and 19).

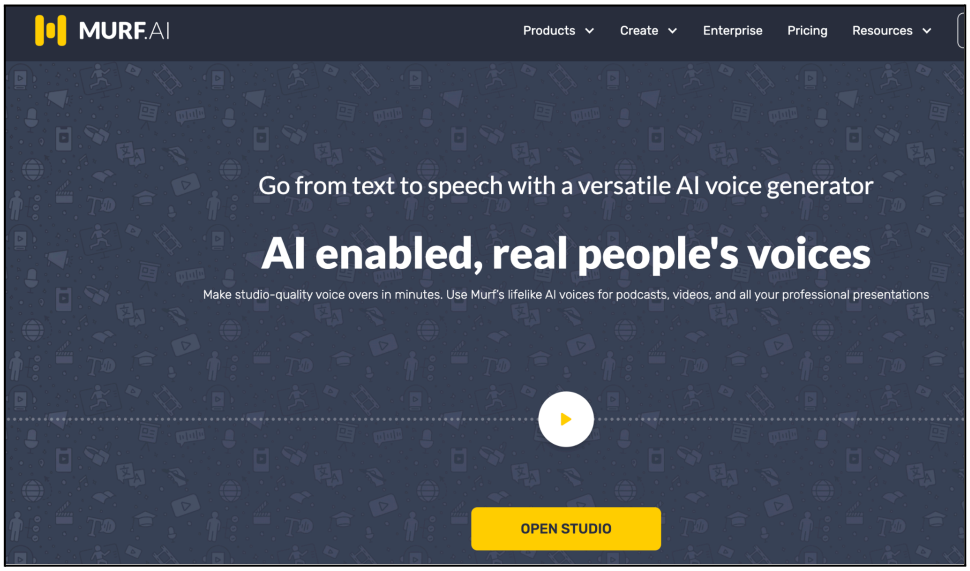


Figure 18 - AI voice software generator (Source: Murf.ai)

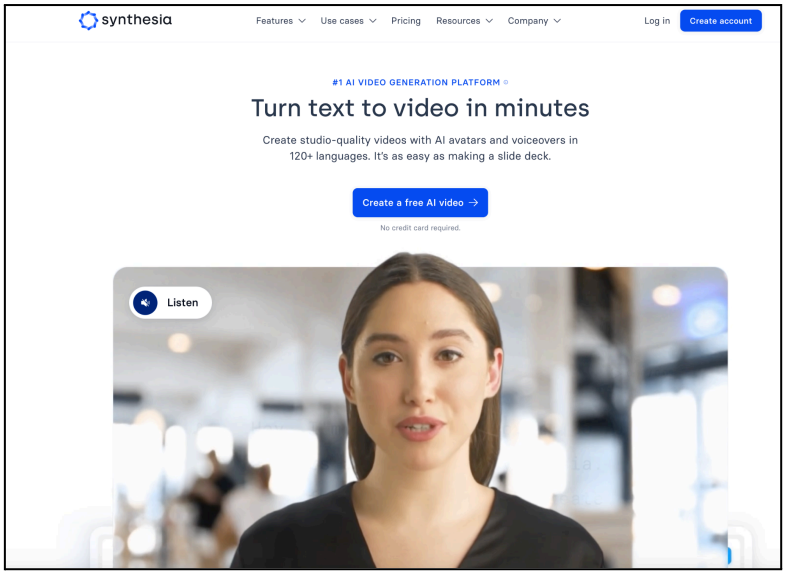


Figure 19 - AI avatar creation software voice and face for videos (Source: Synthesia)

Moreover, AI became a subject of significant interest within the cybercriminal community, which seeks to use it for illicit purposes, including social engineering aimed at deceiving the victim through voice and visual impersonation. of somebody. (Figure 20)



Figure 20 - A threat actor asking on a cybercrime forum about using AI for a Vishing attack (Source: Exploit. in)

The use of AI in attacks aimed at tricking the victim into believing that the person on the other end of the line or in the video is the same person is commonly called “Deepfake.” Deepfakes are photos and videos manipulated using AI to make people appear to be saying or doing something they never did or appear to be in places where they have not been. Deepfake's quality can vary depending on the tools used and the time spent working on the image or video created (Figure 21).

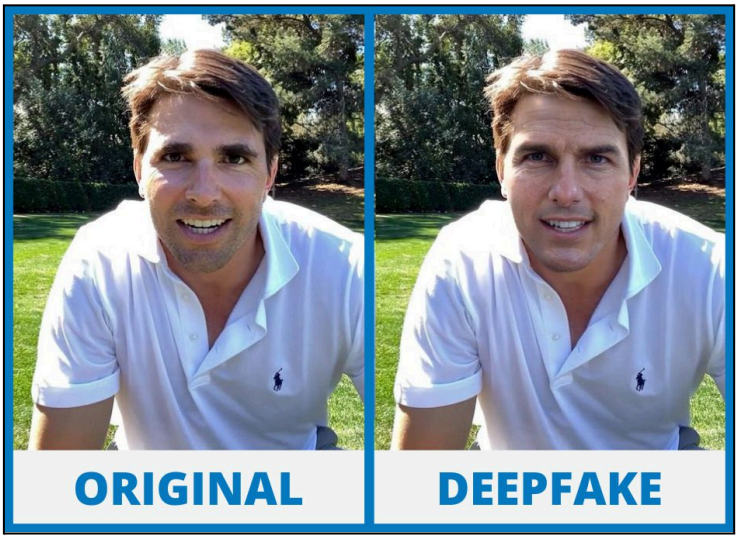


Figure 21 - Real and AI-generated images (Source: Maverick)

There are several types of DeepFake, such as Textual, Audio, Video, Social Media, and Live or real-time (Figure 22).

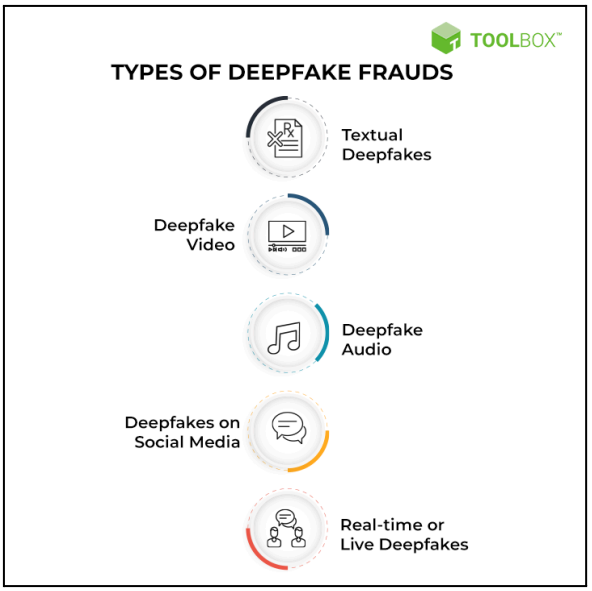


Figure 22 - Different types of DeepFake (Source: ToolBox)

If a DeepFake relies on AI, machine learning is essential in its creation. Convolutional neural networks (CNN) are a subset of powerful AI built in part on the human mind, capable of detecting trends in information, and can be used for image and speech recognition. Creating a deepfake video can be defined as follows:

- First, a large amount of actual video footage must be sent to a deep neural network, which is gradually trained to recognize a person's rhythms and detailed characteristics. This gives the algorithm a realistic representation of an individual's appearance from different perspectives.

- Secondly, it combines with the learning algorithm facial and vocal models generated by the AI obtained from the neural input of the network.

While many think creating a deepfake requires complex tools and technical skills, this is untrue. They can also be created with basic knowledge of computer graphics, which can help to democratize the use of deepfakes. Thanks to advances in AI, deepfakes have become more convincing than ever and are often used to fool people. Some deepfakes look realistic, so it's no surprise that criminals misuse this technology in inventive ways to facilitate scams. Indeed, thanks to AI software like the one presented above, it is possible today and will be even more possible in the long term to impersonate a person's vocal and physical identity and make them say or do what they want. In the coming years, if appropriate security measures are not found and implemented, AI will make manipulating people even more critical, which could lead to a sharp increase in scams, influence campaigns, and illegal activities. Spying.

3.3 Virtual HUMINT

Virtual HUMINT involves using traditional HUMINT techniques and methodologies combined with IT tools and skills to identify, recruit, manipulate, and collect information about sources or targets operating online. Virtual HUMINT is an intelligence discipline using several techniques, including social engineering, as explained previously, as well as negotiation and natural language processing (NLP) techniques. Virtual HUMINT requires a good, in-depth understanding of the world of human intelligence and psychology, as well as cyberspace and its elements. Many threat actors operating in different worlds, including terrorism, criminals, espionage, hacking, and fraud, use virtual HUMINT to carry out their online operations using different levers in human interaction through the Internet. The success of a virtual HUMINT operation generally relies on the human factor.

When a threat actor carries out an online undercover operation, he must first have a minimum of information about his target and clearly define his objectives. Within a second, he can establish contact with his target and get him to do or give him what he wants. However, for this, you must first be able to create a credible contact vector based on the legend you wish to invent. The invention of a legend for an online operation varies from one activity to another. However, the common vector must be sufficiently credible and solid to deceive the victim properly. Many cyber operations, whether cybercriminal, cyber espionage, influence, or terrorist, are carried out mostly through social networks such as Facebook, LinkedIn, and Instagram or encrypted chat applications such as WhatsApp and Telegram.

As described at the beginning of this document, even if most of the world's population is familiar with social networks, they need to be more experts in detecting shady or completely fake profiles. This is one of these points that many malicious actors exploit by creating fake profiles adapted to the cyber operations they wish to carry out. Some threat actors seek to impersonate important positions within actual companies to increase their credibility (Figure 23).

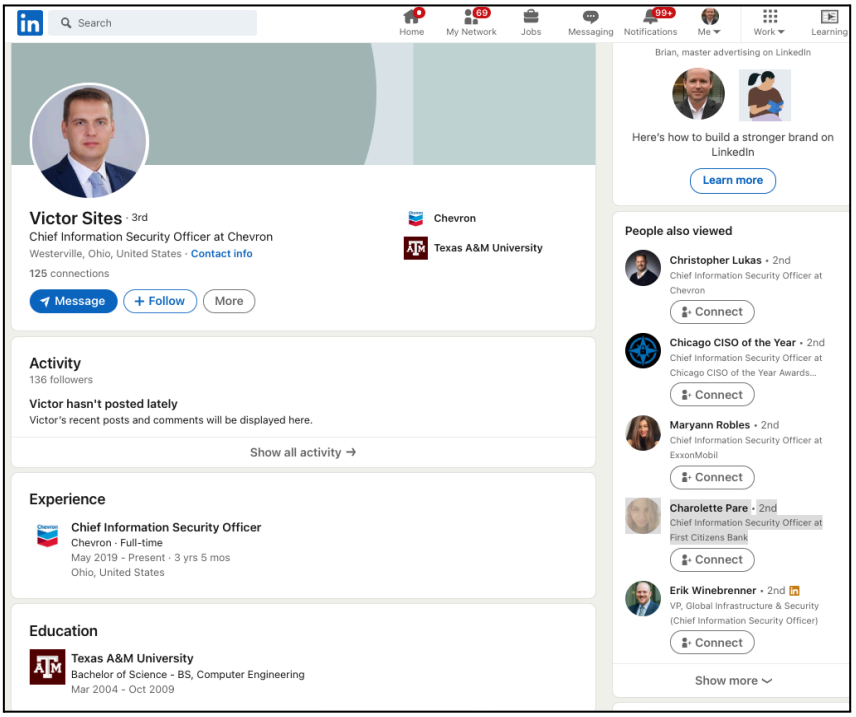


Figure 23 - A fake LinkedIn profile of a person impersonating the position of CISO at Chevron (Source: Brian Krebs).

Such a trick will work on naive people who won't do thorough checks to ensure this person exists on everything if they know they have connections in common. Other threat actors even go so far as to impersonate the profiles of actual people completely. According to the security company Mandiant, hackers working for the North Korean government carried out cyber intelligence operations by copying CVs and profiles from major job boards like LinkedIn and Indeed as part of a well-prepared plan aiming at getting jobs at cryptocurrency companies. Once the profiles and captions are created with varying degrees of professionalism, threat actors usually contact their target with, as mentioned above, a well-defined and credible context and objective (Figure 24).

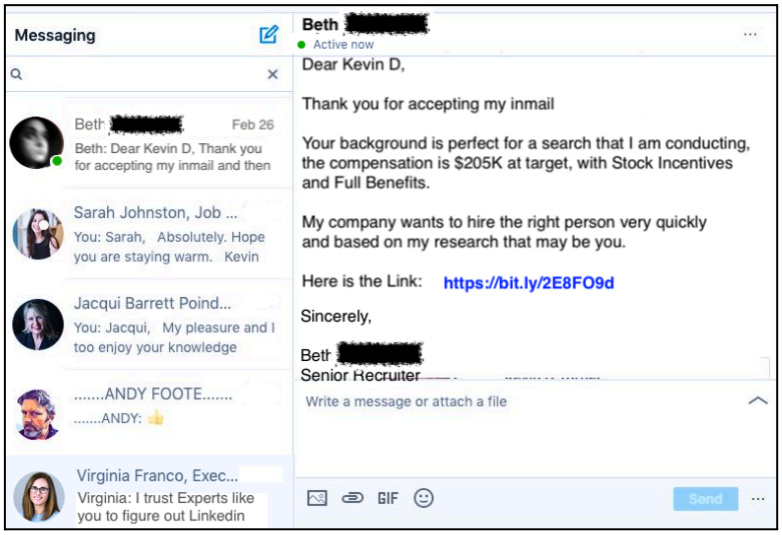


Figure 24 - A Fake Job Offers Spread Malware via LinkedIn Messaging, Invite, & InMail.(Source LinkedIn)

Even if threat actors count on their victim being naive or unaccustomed to new technologies, they can also deceive targets who are supposed to be more aware of online risks. According to the antivirus company BitDefender, this happened in 2022 to a British woman who was said to be a technology expert and aware of online scams (Figure 25). She was duped into transferring almost £16,000 ($21,000) of her savings to fraudsters posing as her daughter on WhatsApp. She declared:

"I received a text message from what I presumed was my daughter, Sam, asking me to delete the old phone number as she'd been given a new number. It went on after a couple of lines of text to ask me if I would make a transaction for her, which I agreed to if she sent me the sort code, the payee's details, and the account number. I presumed it was my daughter, and I thought, well, because of the situation, I was able to do that. Only when Sam didn't reply to say good night, I started suspecting something was wrong."



Figure 25 - WhatsApp conversation between a British woman and a scammer pretending to be her daughter.

Depending on the goal to be achieved (industrial espionage, politics, or financial fraud and scam), threat actors prepare a credible message and adapt it with more or less good language and syntax depending on the threat actors' professionalism level. During a Virtual HUMINT operation, specific message details can be spotted immediately and arouse the target's suspicion, such as spelling errors in syntax or poorly translated expressions automatically and using symbols and smileys. The best Virtual HUMINT operations are generally carried out by actors who master the language, slang, and other specific elements related to the environment of their target, which differ from one country to another even for the same language spoken (e.g., US/UK, Australia/Canada, Spain/Mexico, France/Belgium/Switzerland, Arab countries, etc...).

4. The Human Factor in Cybercrime Operations

In cybercrime, the human factor is an essential, even crucial, element that allows many attacks to succeed. While cybercriminals are developing increasingly sophisticated means and offensive techniques capable of collecting, disrupting, erasing, and encrypting data, network systems, and computers, the success of their attack relies primarily on the human factor. According to the company Proofpoint, Cybercriminals aim mainly at people, rather than IT infrastructures, to install malware, steal data, or initiate fraudulent transactions. In 2023, the company published a report showing that social engineering is a top technique used by cybercriminals (Figure 26).[5]

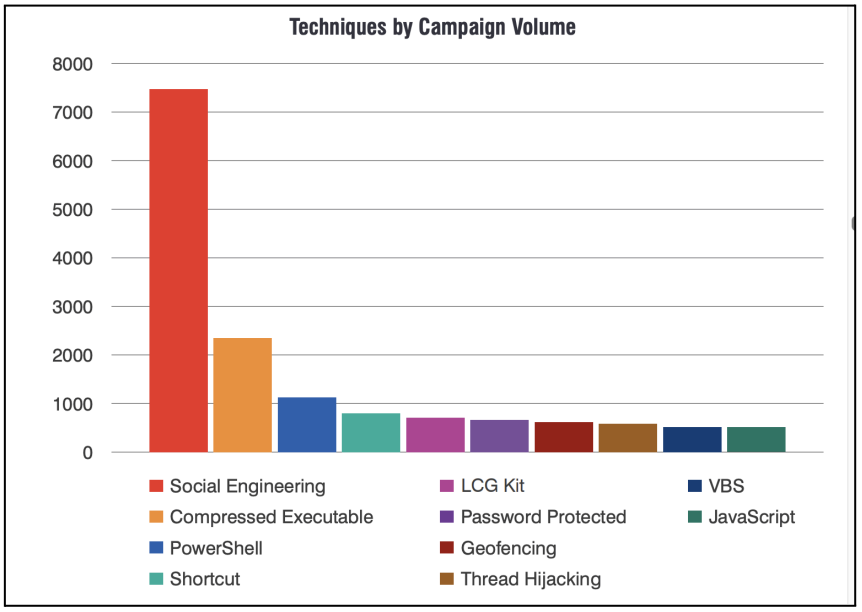


Figure 26 - Attack techniques statistics by volume (Source: Proofpoint)

A joint study by Stanford University and security firm Tessian showed that employee errors cause 88% of data breach incidents. Moreover, another similar study made by IBM Security estimates this number at 95%.[6] The main reasons are usually very weak or non-existent passwords, outdated or insecure software and systems, and a lack of awareness of cyber threats. If a cybercriminal wants to break into a company and introduce malware onto its network, they will tend to do so through people with poor or almost no knowledge of cyber threats, such as secretaries, assistants, accountants, or any other general position in the company, rather than target people from the IT or security department who are expected to be much more savvy and aware of cyber threats.

[5] https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf
[6]https://securitytoday.com/articles/2022/07/30/just-why-are-so-many-cyber-breaches-due-to-human-error.aaspx#:~:text=Let's%20start%20with%20a%20statistic,are%20caused%20by%20employee%20mistakes.

As previously observed, social engineering and virtual HUMINT are related techniques often used by cybercriminals in their operations. The victim, being the weakest point because he is human and therefore sensitive to the emotions of fear, stress, fatigue, lack of attention, or others, is essentially the key to the success of these attacks. Cybercriminals understand this human aspect well and use it constantly. One of the most effective means is to carry out central awareness and training campaigns on cyber threats for public and private sector employees. If implementing cybersecurity system policies and software updates is very important, training employees and customers undoubtedly remains the most effective way to reduce the risks of cyber attacks and fraud.

5. The Human Factor in Cyberwarfare and Influence Operations

Regarding cyberwar, the human factor is also a key element. In recent years, multiple government-linked APT groups have conducted numerous cyber-intelligence operations. One of the most common modes of operation is the creation of fake profiles on professional and personal social networks to approach their targets, contact them, and generally manipulate them to infect their computer or smartphone with spyware. In 2023, Proofpoint revealed that in Pakistan, a state-linked hacking group carried out a cyber intelligence operation on Indian military personnel and the Pakistan Air Force using fake apps and websites to compromise their devices.[7]

The social engineering technique through social networks combined with virtual HUMINT is a widespread technique within these APT groups. Preparing such cyber operations generally requires a certain amount of preparation time to be as credible as possible without arousing the target's suspicion. So, these state groups generally invest time in creating fake profiles and cover stories. Depending on the type of campaign. Cyber espionage generally targets valuable people such as university researchers, senior civil servants, senior managers of financial or political institutions, businessmen, and managers of large companies. On professional social networks such as LinkedIn, target manipulation generally relies on a link between the target and the threat actor using an element familiar to the victim. Threat actors also seek to make their profiles credible by having standard connections to generate trust in the victim. An example of this type of operation is attributed to Chinese intelligence services. In August 2023, the Times revealed extensive use of LinkedIn by a Chinese intelligence officer to target British officials. this spy tricked thousands of officials, scientists, and academics into handing over state secrets and sensitive technological information (Figure 27).

[7] https://therecord.media/pakistan-india-cyber-espionage-meta-bahamut-patchwork



Figure 27 - Fake LinkedIn profile operated by a Chinese threat actor (Source: The Times)

When they operate on more personal social networks like Facebook or Instagram, threat actors tend to play on the seduction effect by using profiles of attractive young girls to attract the attention of their target. In the context of the cyber war between Israel and Hamas, cyberespionage tactics used by Iran include the creation and use of numerous fake profiles of attractive Hebrew-speaking women to gather intelligence from Israeli soldiers (Figure 28).

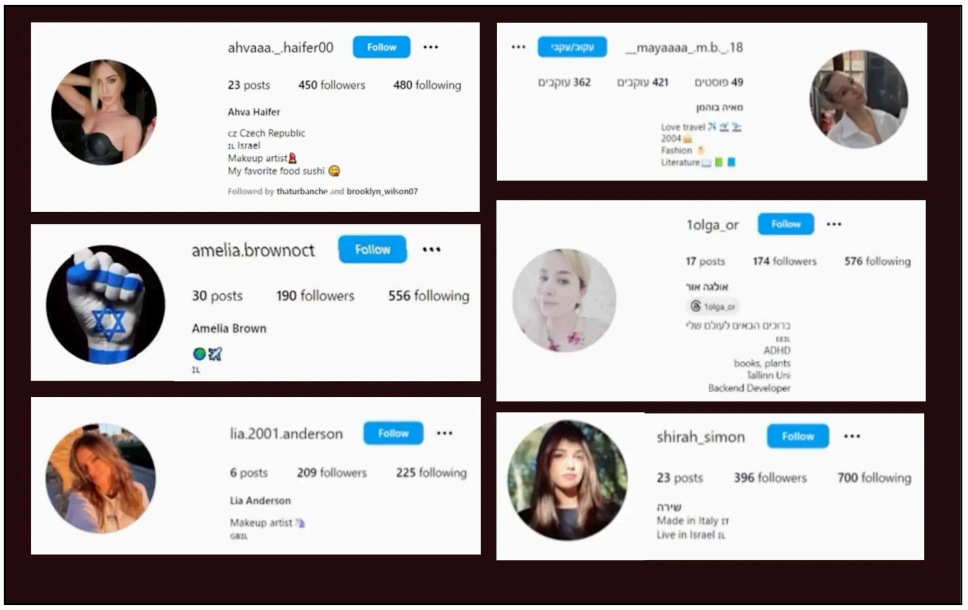


Figure 28 - Fake Instagram profiles created by Iranian Hackers to obtain information from Israeli soldiers (Source Iran International)

Cyberwar is also a war of information or rather of disinformation and influence. Threat actors linked to different States have been carrying out campaigns of attempted influence and disinformation for several years. The use of bots and Artificial Intelligence became commonplace, making it possible to increase the strike force by spreading false news or manipulating images or comments. In 2023, US cybersecurity company Mandiant claimed it had seen an increase in the use of AI to carry out manipulative information campaigns online in recent years. The company's researchers say that since 2019, a large amount of AI-generated content, such as fabricated profile photos, has been used in politically motivated online influence campaigns. According to a report published by Mendiant, this phenomenon seems global because these campaigns are carried out by groups aligned with the governments of countries like Russia, China, Iran, Ethiopia, Indonesia, Cuba, Argentina, Mexico, Ecuador, and El Salvador. Among these countries, China and Russia are arguably the most active in creating false narratives and profiles, as well as media spoofing for disinformation and influence of foreign countries. They often use AI to create fake profiles, posting images and content that are erroneous, diverted, or simply false (figures 29 and 30).



Figure 29: AI-generated image posted by suspected Chinese IO assets (Source: Microsoft)

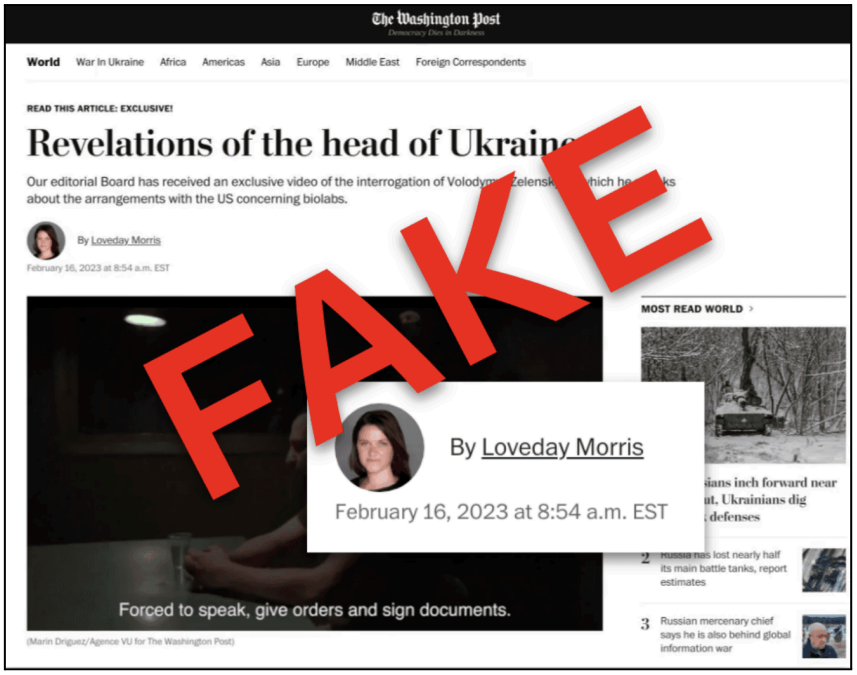


Figure 30 - An example of a fake article created by Russia and impersonating the Washington Post (Source: Meta)

They use different techniques to manipulate information and images, sometimes using fear of threat, denial, and denigration (Figure 31).

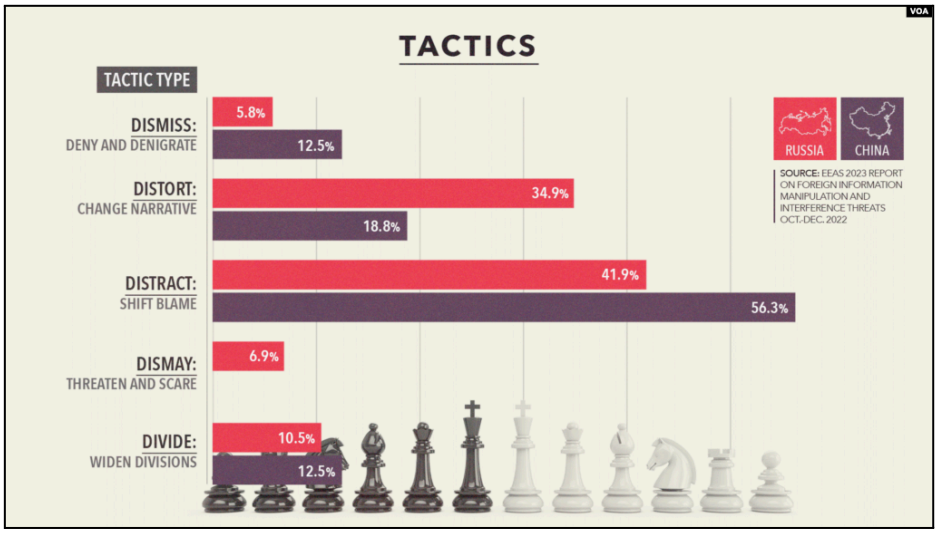


Figure 31 – Tactics used by Russia and China in disinformation campaigns (Source: VOA)

6. The Human Factor in Cyber Terrorism Operations

Cyberterrorism can be defined as using technology and cyber means to terrorize a civilian population, influence government policy, or target critical state infrastructure for religious or ideological purposes. For several years, terrorist groups like Hamas, Hezbollah, and the Islamic State have exploited the human factor during their cyber operations to achieve their objectives. From ideological propaganda to psychological warfare to the manipulation and deception of people to recruit online or infect targets with spyware, the human factor is at the heart of terrorist groups' cyber operations.

One of the preferred means of these terrorist groups to approach their target in a cyber intelligence operation is the creation and use of fake Facebook or Instagram profiles of attractive young women. This technique allows them to initiate a conversation with a male target, often a soldier or senior military and political official, to manipulate them and get them to click on a link leading them to download spyware.

In 2022, according to research performed by the cybersecurity firm Cybereason, a Hamas-linked attack group, APT-C-23 (AKA Arid Viper, Desert Falcons), was involved in a sophisticated intelligence-gathering campaign targeting senior Israeli officials. Beyond social engineering using fake Facebook accounts, the group introduced new malware, including a fake messaging app known as VolatileVenom, a downloader known as Barbie Downloader, and theBarbWire Backdoor (Figure 32).

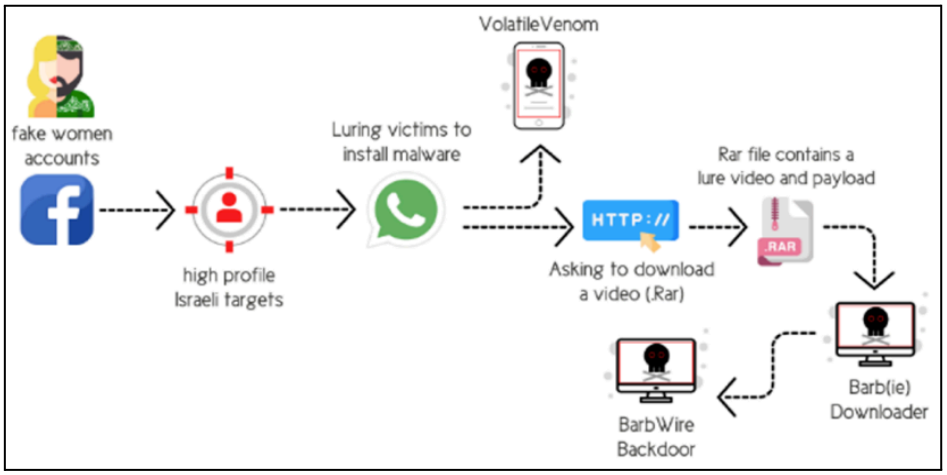


Figure 32 - Hamas Volatile Venom malware infection method (Source: Cybereason)

In 2022, it was revealed by The Times that the terrorist organization Islamic State was using fake profiles on the dating app Tinder to attempt to approach and blackmail South Africans into funding the presence of the Islamic State. organization in Africa. Fake profiles, created by Islamic State militants, used photos of models and lesser-known actresses to target South Africans by asking them to share intimate photos of themselves. The profiles use these photos to blackmail individuals, demanding payments that would then be given to Islamic State leaders.[8]
Amid the tense geopolitical context in the Middle East, according to a recent Google report, hackers linked to Iran and the terrorist group Hezbollah have carried out cyber operations aimed at undermining support and influencing public opinion on the war between Israel and Hamas. Whether Hamas, Hezbollah, or the IRGC, terrorist cyber operations aimed at gathering intelligence, influencing, or supporting the population have increased considerably since October 7, 2023. Human manipulation through deception with false profiles and the dissemination of false images is now an integral part of the modus operandi of terrorist groups. Terrorist groups have well understood the psychological impact of such cyber operations on populations. This impact of psychological manipulation is also illustrated in the use of AI by terrorist groups. Since October 7, numerous fake news and AI-generated images have been distributed on social media (Figure 33).



Figure 33 - Fake image released by pro-Hamas and generated with AI system

[8] https://www.jpost.com/international/article-722566

7. Conclusion

As reviewed and analyzed in this document, the human factor plays an essential role in the success of cyber operations initiated by different threat actors. It is the entry point to the digital infrastructure of a public organization, a government, or a private company. Whether using social engineering, virtual HUMINT, or AI, threat actors understand how to manipulate targets using psychological levers, allowing them to deceive their victims and lead them to carry out malicious actions for their benefit.

Human vulnerability is and will always remain the most critical point, so it is essential, if not crucial, to always be informed, trained, verified, compare, and question everything going through cyberspace. As mentioned earlier, while governments and businesses use many sophisticated security systems to counter and protect various infrastructures around the world, they can only be truly effective if, on the one hand, they learn about external threats through cyber intelligence means, but more than anything if the people working in these private or public institutions are trained to recognize and anticipate cyber threats. Training people, regardless of their hierarchical or technical level, is one of the keys to success in the fight against cyber-attacks, fraud, and online misinformation.

8. About The Author

I am a cyber intelligence expert who has worked in various environments over the past ten years, including academia, high-tech, military, and law enforcement. My field of expertise is cyber intelligence, including strategy, collection, research, analysis, and leading Cyber HUMINT operations on criminal and terrorist activities within cyberspace. I have trained many civilian analysts and Military and Law Enforcement officers on the Deep and Dark Web environments, Cyber intelligence collection, and Cyber HUMINT operations.

