

Bachelor's Thesis

Business Information Technology

2022

Kim Rosengren

Contribution of Open-Source Intelligence to Social Engineering Cyberattacks



Bachelor's Thesis | Abstract

Turku University of Applied Sciences

Business Information Technology

2022 | 47 pages

Kim Rosengren

Contribution of Open-Source Intelligence to Social Engineering Cyberattacks

The majority of cyberattacks occur without the need to break into IT systems. Attackers use psychological methods and exploit readily accessible information to manipulate their targets into making irrational decisions. The primary intent of this thesis was to assemble a literature review that provides the fundamental comprehension of social engineering attacks and open-source intelligence. The main goal was to determine why social engineering attacks are so prevalent and what role open-source intelligence plays in them. The scope of the review was limited to the most common techniques, methods, and tools. The research method was primarily qualitative, containing references gathered from reputable web sources and relevant literature. The study findings showed that predictable emotions and behavioural patterns make humans the most vulnerable aspect of cybersecurity and that information is a crucial element of influence. Therefore, the most effective social engineering defence approach is to educate web users about online privacy protection and how to recognise and respond to attacks.

Keywords:

cybersecurity, information security, open-source intelligence, social engineering

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tietojenkäsittely

2022 | 47 sivua

Kim Rosengren

Avointen lähteiden tiedustelun rooli sosiaalisen manipuloinnin kyberhyökkäyksissä

Useimmat kyberhyökkäykset tapahtuvat ilman murtautumista tietojärjestelmiin. Hyökkääjät käyttävät psykologisia menetelmiä ja helposti saatavilla olevaa tietoa manipuloidakseen kohteitaan toimimaan harkitsemattomasti. Opinnäytetyön päättämiseksi oli koota kirjallisuuskatsaus, joka antaa kattavan perusymmärryksen sosiaalisen manipuloinnin hyökkäyksistä ja avointen lähteiden tiedustelusta. Tavoitteena oli selvittää, miksi sosiaalisen manipuloinnin hyökkäykset ovat niin yleisiä, ja mikä on avointen lähteiden tiedustelun rooli niissä. Opinnäytetyö rajattiin tarkastelemaan vain yleisimpiä menetelmiä ja työkaluja. Työssä käytettiin pääasiassa kvalitatiivista tutkimusmenetelmää, ja tutkimusaineisto koostui luotettavista verkkolähteistä ja relevantista kirjallisuudesta. Katsauksessa todettiin, että ennustettavat tunnetilat ja käyttäytymismallit tekevät ihmisestä kyberturvallisuuden heikoimman pisteen, ja että informaatiolla on tärkeä rooli vaikuttamisessa. Näin ollen, tehokkain puolustuskeino sosiaalista manipulointia vastaan on opastaa verkon käyttäjiä suojaamaan yksityisyyttään, tunnistamaan hyökkäykset ja reagoimaan niihin.

Asiasanat:

avointen lähteiden tiedustelu, sosiaalinen manipulointi, tietoturva

Content

List of Abbreviations	6
1 Introduction	7
2 Social Engineering	9
2.1 History	10
2.2 Psychology	11
2.3 Attack Methods	15
2.3.1 Phishing Attacks	15
2.3.2 Other Attacks	17
3 Open-Source Intelligence	20
3.1 Malicious Utilisation	21
3.2 Advantages, Disadvantages and Concerns	23
3.3 Resources, Tools, and Techniques	24
4 Notable Incidents	37
5 Countermeasures	41
5.1 Individuals	41
5.2 Organisations	42
5.3 Phishing Warning Signs	42
6 Conclusions	43
References	44

Figures

Figure 1. Phases of Social Engineering (Salahdine & Kaabouch, 2019).	10
Figure 2. Principles of Persuasion (Cialdini, 2021).	12
Figure 3. OSINT Sources (Bazzell, 2022; Hassan & Hijazi, 2018).	21
Figure 4. OSINT Exploration Example (Beffa, 2020).	22

Figure 5. Connected IoT Devices 2019-2030 Forecast (Statista, 2022b).	23
Figure 6. Layers of the Internet (Hassan & Hijazi, 2018).	24
Figure 7. A Fraction of the OSINT Framework. (Nordine, n.d.)	26
Figure 8. Google Dorking.	27
Figure 9. Shodan Search.	29
Figure 10. The Internet Archive.	31
Figure 11. The Wayback Machine Search.	31
Figure 12. Spokeo Name Search.	32
Figure 13. PeekYou Username Search Results.	32
Figure 14. Have I Been Pwned Results.	33
Figure 15. Pics2Map EXIF Extraction.	34
Figure 16. Hunter Search.	35
Figure 17. Whois Domain Information.	36
Figure 18. Twitter Bitcoin Scam.	39
Figure 19. Vastaamo Ransom Message (Aves Netsec, 2020).	40
Figure 20. Vastaamo Patient Ransom Message (Aves Netsec, 2020).	40

Tables

Table 1. Popular Google Commands and Operators.	28
---	----

List of Abbreviations

2FA	Two-Factor Authentication
AI	Artificial Intelligence
CD-ROM	Compact Disc Read-Only Memory
COVID	Corona Virus Disease
DNC	Democratic National Committee
EXIF	Exchangeable Image File
GPS	Global Positioning System
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
OSINT	Open-Source Intelligence
SOCMINT	Social Media Intelligence
UN	United Nations
URL	Uniform Resource Locator
USB	Universal Serial Bus
VHS	Video Home Systems

1 Introduction

The Internet revolutionised the world by making communication and information sharing more efficient. However, as technology advances and the amount of publicly available data expands, web users become more vulnerable to cybersecurity threats. By April 2022, the internet had reached 63% of the world's population, totalling five billion individuals, of which 4.65 billion use social media. (Statista, 2022a)

The COVID-19 epidemic accelerated online data growth by restricting in-person social activities, and a lack of preparation for remote work may also have contributed to a significant rise in cybercrime. In May 2020, UN Disarmament Chief Izumi Nakamitsu confirmed a 600% growth in malicious emails. Recent statistics suggest that 98% of cyberattacks involve social engineering elements. Even organisations with advanced security systems are vulnerable because technology cannot prevent social engineering cyberattacks from succeeding. (CompTIA, n.d.; Galov, 2022; The Associated Press, 2020)

Since Russia's invasion of Ukraine began in February 2022, "information warfare" and "cyberwarfare" have become mainstream buzzwords. Thanks to social media, the current war is almost certain to be the most well-documented in history. When information can reach billions of people instantly, it is not surprising that cyberattacks and influence methods such as disinformation, social engineering, and propaganda may be involved. Wars may appear predictable from a technical standpoint, but the human element can greatly influence events. (Zarembo & Solodkyy, 2021)

This paper aims to offer a comprehensive overview of social engineering, an approach to conducting cyberattacks involving psychological influence, and open-source intelligence, a powerful information gathering method. The main objectives of this review are to explore the fundamental concepts of these two subjects and understand their interrelationship better.

Later chapters will also explore open-source intelligence by assessing practical techniques and tools, present some significant social engineering incidents, and suggest a few defensive measures.

This is not a practical handbook for performing social engineering attacks or gathering information. The study's findings are intended to assist ordinary web users and organisation members in identifying and responding to these types of cyberattacks, recognising the value of all kinds of personal information, and taking measures to secure their privacy and data.

2 Social Engineering

Social engineering refers to human interaction techniques utilised since the beginning of civilisation. Any behaviour with the intent of influencing someone to act against their own best interests is viewed as social engineering. It is more commonly known as manipulation in everyday life. Social engineering cyberattacks are typically motivated by data, money, or access. However, this does not imply that social engineering is only used for malicious purposes. Government agencies, organisations and cybersecurity professionals often utilise social engineering in criminal investigations, security protocol testing and other legitimate purposes. For instance, The Innocent Lives Foundation (*innocentlivesfoundation.org*) is a non-profit organisation dedicated to rescuing children from predators. The foundation works with law enforcement and consists of cybersecurity experts who use social engineering and open-source intelligence to uncover predators. (Hadnagy, 2018)

Social engineering techniques are widely used in cyberattacks because exploiting the human mind is simpler than penetrating modern IT systems. This is achieved by incorporating psychology and gathered intelligence to manipulate human behaviour through emotions and trust. Although social engineering can be done in person, cybercriminals typically use communication devices to attack multiple targets simultaneously. Social engineering cyberattacks are relatively inexpensive to execute, requiring only a computer or a smartphone with internet access. Compared to in-person crimes, the potential rewards are enormous, and the risk of being caught is minimal. Because there are numerous attack methods and no standard way to execute them, a well-executed attack is difficult to detect. They differ depending on the scenario and intelligence. However, attacks typically follow a pattern with four primary phases (Figure 1): research, hook, play, and exit. (Hadnagy, 2018; Salahdine & Kaabouch, 2019)

PHASES OF SOCIAL ENGINEERING



Figure 1. Phases of Social Engineering (Salahdine & Kaabouch, 2019).

Starting with the Research phase, the attacker gathers information about the target and plans the attack. During the Hook phase, they create pretext scenarios based on the intelligence gathered and begin to build a relationship with the target. During the Play phase, the attacker psychologically manipulates the target into disclosing sensitive information or making security errors. Finally, during the Exit phase, they stop engaging with the target and clean up any potential traces. (Salahdine & Kaabouch, 2019)

2.1 History

The Trojan War is one of the major events in Greek mythology, and the Trojan Horse is a well-known legend among the public. According to the story, the Trojans and the Greeks were at war in 1184 B.C., and after a 10-year siege, the Greeks had to get creative in defeating the Trojans. They built a giant wooden

horse and hid some of their warriors inside. The rest withdrew and sailed away, acting defeated. The Trojans were deceived and took the wooden horse beyond their protective walls. When the Trojans went to sleep, the Greek warriors exited the wooden horse and opened the city's gates, allowing in the rest of their army, who had returned quietly in the dark. The Greeks then used the element of surprise to destroy Troy from within.

The Greek legend is frequently cited as the first known instance of social engineering, "occurring" long before the information age and even inspiring a malware category (Trojan horse, malware that conceals its real motive). While deception has probably existed since the dawn of civilisation, it was not until thousands of years later that this type of deception was given a name in cybersecurity. The Dutch entrepreneur J.C. Van Marken first introduced the term "social engineering" in 1894 to highlight the need for professionals to manage human challenges. In 1911, American sociologist Edwin Lee Earp published his book, *The Social Engineer*, urging people to approach social interactions as they approach technology. More recently, the term has been redefined to refer to the process of persuading people to act against their own best interests. Kevin Mitnick, a former cybercriminal, popularised this concept in the cybersecurity community in the 1990s, and it has since been used mainly in this context. (CompTIA, n.d.)

2.2 Psychology

Social engineering attacks rely on psychological exploits to succeed. Social engineers understand how humans make decisions, and they manipulate the circumstances to persuade their target to make a poor choice. Some individuals are more prone to influence than others, but rarely because they are unintelligent or gullible. When their emotional triggers get exploited, even the most cautious and intelligent people tend to react without thinking if they are not aware of these manipulation tactics. Attackers take advantage of human emotions, including fear, trust, curiosity, urgency, and greed. (Hadnagy, 2018)

Dr Robert Cialdini is the leading expert on the psychology of influence. The six main principles of persuasion (Figure 2) defined in his book *Influence: The Psychology of Persuasion* are frequently applied in various professional environments and marketing campaigns. Social engineers' most common psychological techniques are based on the same principles.

PRINCIPLES OF PERSUASION

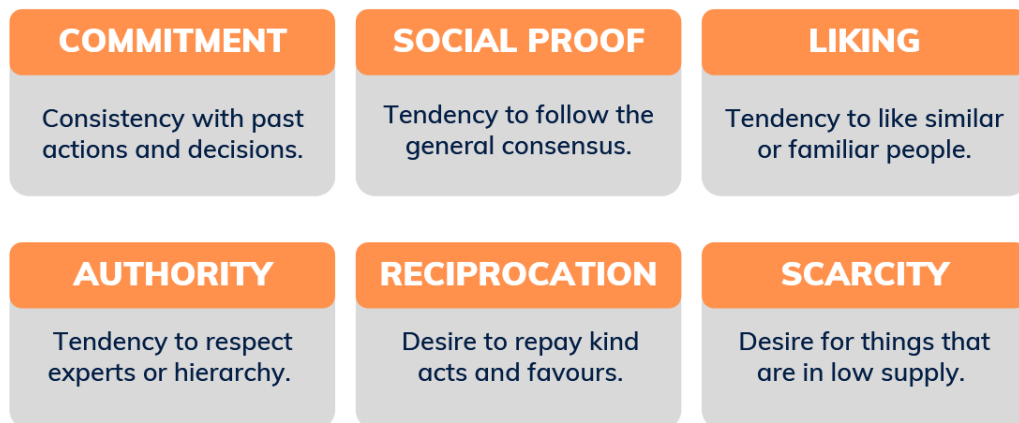


Figure 2. Principles of Persuasion (Cialdini, 2021).

Liking and Familiarity

People are more likely to comply with requests made by people they know and like. People often like someone they find attractive, similar, familiar, or relatable. This explains why celebrity endorsements are so influential. (Cialdini, 2021)

Liking is a powerful and versatile technique that social engineers frequently use. The possibilities are almost endless. It is an effective method for building rapport with the target, but it can also be used for direct attacks if the target's interests are known. (Talamantes, 2014)

Reciprocation and Obligation

Most of the time, people want to repay those who do something nice for them. Compliance can be effectively gained using reciprocity. It can produce a favourable response to a request that would most probably be denied without a sense of obligation. (Cialdini, 2021)

Because most people feel obligated to repay someone for a favour, gift, invitation, or kind gesture, malicious attackers often offer their target something they know will be appreciated and later make their request when the target is more prone to oblige. Even a simple compliment can make the target more willing to open up and reveal information. Informing the target that they have won something that has to be shipped or providing a refund on a service that requires further banking details for deposit is a standard method to gather address or credit card information. (Hadnagy, 2018)

Social Proof and Consensus

Peer pressure and herd behaviour are both examples of social proof. People base their decisions on the actions and opinions of others. They believe that if multiple people agree on something, it must be a safe or sensible decision. (Cialdini, 2021)

Social engineers use social proof to convince their targets that the decision they are about to make is a good one. For instance, fake product reviews are used on fraudulent websites to persuade targets to buy a product they will never receive. Another common social proof application is to inform the target that their peers complied with the requests. This is frequently used on company employees who are reluctant to share information. It is especially effective when combined with authority. (Mitnick Security, n.d.)

Commitment and Consistency

People want to appear consistent with their previous decisions. Once they have made a decision or taken a stand, they will be under pressure to follow through on that commitment. They will attempt to stay consistent with their previous commitments. (Cialdini, 2021)

Requests that are consistent with previous commitments are more likely to be accepted. Attackers more commonly use this approach to build rapport with the target over time, beginning with a small request and escalating to a larger request later when more trust has been established. Consistency compels the target to stay committed and maintain their self-image. (Mitnick Security, n.d.)

Authority

Children are taught to respect their parents, teachers, and the elderly from an early age. Those individuals commonly grow up to be adults who instinctively respect and obey authority figures, such as law enforcement, bosses, experts, and people of higher social status. (Cialdini, 2021)

People are far more likely to follow instructions given by someone in a position of authority, legitimate or not. Attackers impersonating authority figures may exploit the target's desire to be liked or desire to comply for potential benefits or out of fear. (Talamantes, 2014)

Scarcity and Urgency

People are more interested in things that are limited in supply. Scarcity, or its illusion, is a powerful motivator for human behaviour. People desire things they cannot have or believe they will not be able to obtain unless they act quickly. This is the most used applied sales approach. (Cialdini, 2021)

Scarcity is used in social engineering attacks to create a situation or feelings of urgency, pushing the target to make a hasty decision. Fraudulent offers and opportunities are frequently used to obtain information or execute direct attacks. Scareware and ransomware attacks often use intimidation to create a sense of anxiety, fear, and urgency. (Talamantes, 2014)

2.3 Attack Methods

There are various ways to execute social engineering attacks. It can be done online, on the phone, or in person. One of the most popular methods is text-based phishing because it can be sent to multiple targets simultaneously, and the attacker does not have to interact with the target. The pay-out potential is enormous, and the attacker does not need the solid social skills required for live calls and in-person impersonation.

According to Cisco's 2021 Cybersecurity Threat Trends report, phishing attacks are involved in 90% of data breaches. Attacks can include fraudulent websites, emails, advertisements, scareware, banking websites, free offers, IT support, and others. They typically attempt to gain personal information from their targets using social engineering. Such information may include credit card information, insurance information, full name, physical address, pet's name, first job, mother's family name, place of birth, visited places, and so on. Combining several attack types is common for increased effectiveness. (Cisco, 2021; Salahdine & Kaabouch, 2019)

2.3.1 Phishing Attacks

Phishing occurs when an attacker poses as a trustworthy source and tries to persuade their target into revealing information or clicking a malicious link that installs malware. Successful attacks can lead to compromised systems, data theft, and financial loss. Phishing can be a mass operation where the attacker intends to harvest passwords or make fast profits, or it can be the first step in a

targeted attack against an organisation or individual with a more specific goal, such as stealing sensitive data. The attacker may use information about the employees or company in a later targeted phishing attack to make their messages more believable. (National Cyber Security Centre, 2018)

Text-based Phishing

Phishing is mainly done through email, text messages (SMiShing), or social media. Phishing emails can reach millions of people and blend in with the many harmless emails that people receive daily. Attackers send emails, texts, or social media messages impersonating a known sender and using social engineering techniques to create a sense of urgency and deceive their targets into clicking on a link or downloading an attachment. Traditionally, the links lead to malicious websites that steal credentials or install malware on the target user's device. The attached documents contain malicious content that installs malware when the user opens them. (Panda Security, 2021)

Spear Phishing and Whaling

Spear phishing is targeted and personalised phishing. Instead of sending mass emails to thousands of people, spear phishing targets a specific individual or organisation, often with content tailored to the victim to make them believe they have a relationship with the sender. Attackers frequently use open-source intelligence to gather relevant information (e.g., the target's co-workers, positions, and professional associations) to assist them in their attack. Whaling is like spear phishing, but instead of targeting low-level targets, attackers go after "the big fish" or "the whale." CEOs, CFOs, and other high-level executives with access to more sensitive data than lower-level employees fall into this category. Whaling can also target other high-profile individuals, such as celebrities and politicians. (Malwarebytes, n.d.)

Vishing

Vishing stands for "Voice Phishing." Targets are exploited via voice calls rather than text messages. A vishing call may use live human operators or an automated voice message from what appears to be a legitimate institution, such as a bank or a government department. Because the call creates a sense of urgency and demands immediate interaction, the recipient is easily tricked into sharing personal information. (Panda Security, 2021)

2.3.2 Other Attacks

Scareware

Scareware is a type of online fraud that uses pop-up advertisements to scare people into downloading or purchasing fraudulent cybersecurity protection software that turns out to be useless or malicious malware. A typical scareware pop-up usually informs the user that their computer or files have been infected and then offers software that claims to fix the problem. Scareware can also be spread via spam email as messages that persuade users to purchase other useless products or services. (Buxton, 2021)

Ransomware

Ransomware attacks install malicious malware that encrypts the target's data, limiting access to it. The attacker then attempts to extort the target by demanding a ransom for data access. If the ransom is not paid, the files will be destroyed or made public. This payment is usually requested in cryptocurrency, an unregulated digital currency that is difficult to track. Access to the files will not be guaranteed even after payment. (Salahdine & Kaabouch, 2019)

Pretexting and Impersonation

Pretexting means creating fictional and believable scenarios to gain the target's trust. Impersonation involves assuming a false identity to go along with the story. Successful attacks most often require previous research on the target and the use of this intelligence for execution. Pretexting attacks are highly effective and common both online and offline because it is now easier to stalk people on social media and develop a believable pretext. This technique needs a certain amount of creativity, but the possibilities are endless. Attackers may impersonate law enforcement, relatives, banks, co-workers, tax authorities, and anyone else with influence on the target. (Salahdine & Kaabouch, 2019)

Baiting

Baiting is a popular method on disreputable websites and social media, where the target is tempted into downloading a media file that turns out to be malware. Emails informing the recipient that they have won a prize are also popular, luring them into clicking a link that leads to a website that requests personal information or installs malware. (Pilette, 2021)

Another type of baiting attack is physical media baiting. The attacker takes advantage of the target's curiosity to tempt them into inserting malware-infected portable media into their computer. Usually, it is a CD-ROM or USB flash drive with a catchy label left somewhere for the target to find or directly handed to them through pretexting and impersonation. Typically, the portable media will launch a malicious program in the background without the target's awareness, allowing the attacker to spy on their computer activities, webcam, microphone, or take control of their computer. (Talamantes, 2014)

Quid Pro Quo

Quid pro quo is a Latin phrase that means "something for something." A quid pro quo attack involves exchanging information for a service or compensation. This sounds like baiting, but instead of tempting someone to take the bait by providing easy access to something they want, attackers offer them something in exchange. The most common quid pro quo attack involves impersonating a company's IT support and requesting additional information from employees to resolve IT problems. (ENISA, n.d.)

Tailgating

Tailgating, sometimes also known as "piggybacking", is a technique that has appeared in numerous films. It involves physically following an authorised individual into a restricted area, usually by impersonating someone who is also permitted or creating a pretext to persuade them. Tailgating attacks are typically directed at large organisations as the possibility of physically getting caught makes them riskier than online attacks. Once entered, the attacker can steal or modify confidential information for malicious reasons and compromise the internal network with malware. (ENISA, n.d.)

3 Open-Source Intelligence

Intelligence gathering is typically associated with government agencies utilising sophisticated tools and classified resources unavailable to the public. In Finland, only the Finnish Security Intelligence Service (Suojelupoliisi) may use invasive surveillance methods, such as telecommunications surveillance and network traffic monitoring, to gather intelligence on civilians. Citizen privacy is protected by law (Police Act, 2011), and surveillance is warranted only when national security is at risk. However, as Edward Snowden's 2013 exposure of a secret US mass surveillance program proved, privacy continues to be a significant concern, even if unwarranted surveillance is illegal. Advanced tools and classified sources are no longer necessary for obtaining valuable personal data, as most of it is easily accessible. (Satter, 2020; Suojelupoliisi, n.d.)

Open-source intelligence (OSINT) refers to collecting and analysing information obtained from publicly available sources for intelligence purposes. For instance, intelligence services may gain valuable information from foreign media, while attorneys can acquire data from legitimate public records. Essentially, OSINT covers all the information that is accessible to the public. (Bazzell, 2022)

Data obtained with OSINT methods can be used for various purposes, including criminal, financial, and terrorism investigations and ordinary activities, such as business competitor research and background checks on potential hires, services, and vendors. According to estimates, OSINT sources provide 90% of the valuable data gained by intelligence services. This makes OSINT a valuable resource even for authorities with access to classified information. One of the significant OSINT sources is social media, as it actively encourages people to share information, resulting in a large amount of user-generated data in one place. Figure 3 presents a variety of OSINT sources. (Hassan & Hijazi, 2018)

OSINT SOURCES



Figure 3. OSINT Sources (Bazzell, 2022; Hassan & Hijazi, 2018).

3.1 Malicious Utilisation

Open-source intelligence is frequently used for malicious purposes as well. Cybercriminals, authoritarian governments, terrorist organisations, and other malicious actors effectively exploit the internet in their operations. OSINT is a vital component of social engineering attacks. Finding enough information to execute a malicious attack is now easier than ever because many may think that sharing certain types of personal information is harmless. However, useful intelligence is not limited to sensitive information, such as credit card numbers and passwords. Even ordinary information, such as a workplace, a particular interest, or a vacation photo, can be useful in a social engineering attack. Sometimes the information is used to execute a direct attack, but it may also be used to get more useful information. Using only one piece of basic information as a starting point (Figure 4), such as a person's real name, username, or email address, OSINT research might uncover private details the target did not know were publicly available. (Beffa, 2020; Hadnagy, 2018)

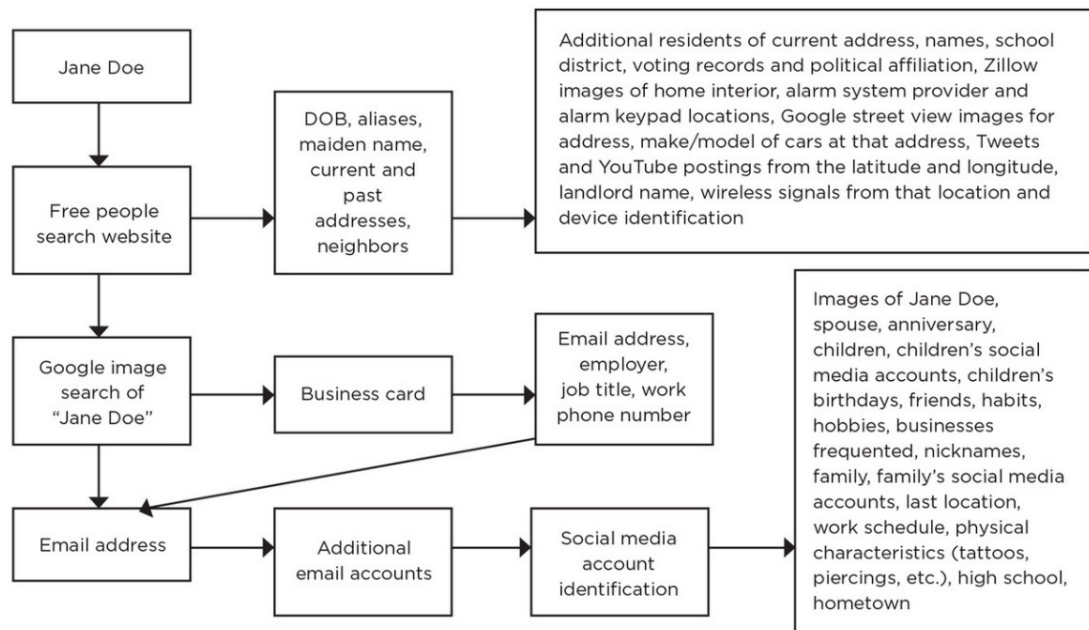


Figure 4. OSINT Exploration Example (Beffa, 2020).

The public domain contains a vast amount of information on individual web users and consumers. It is not complicated to form a comprehensive profile of a person's routines, circumstances, and behaviours by piecing together information from social media profiles, internet activity, public documents, and other OSINT sources. While people have intentionally shared a significant part of their personal information discovered online, they often do so without knowing or understanding the potential repercussions. Additionally, numerous well-known platforms, such as Facebook, Google, Microsoft, Apple, and Amazon, hold massive amounts of user data not meant to be public, including sensitive information such as full names, addresses, phone numbers, credit card numbers, and passwords. Users may believe that their data is secured because the companies are reputable industry leaders. However, organisations of all types and sizes may encounter multiple cyberattack attempts every week. When a data breach occurs, cybercriminals will exploit the data and most likely make it public. (CrowdStrike, 2022; GOV.UK, 2022)

3.2 Advantages, Disadvantages and Concerns

Although open-source intelligence may be gathered online and offline, the most significant portion is already available online as governments, organisations, institutions, and other OSINT providers are rapidly migrating to digital formats. The number of social media users and Internet of Things (IoT) devices (Figure 5) will continue to rise, resulting in a significant increase in the quantity of digital information. Almost all OSINT sources will be available online in the coming years, providing global access to a massive volume of up-to-date information. OSINT gathering is also more economical and less risky than conventional espionage operations that require human sources, advanced equipment and systems, and other expenses. (Hassan & Hijazi, 2018)

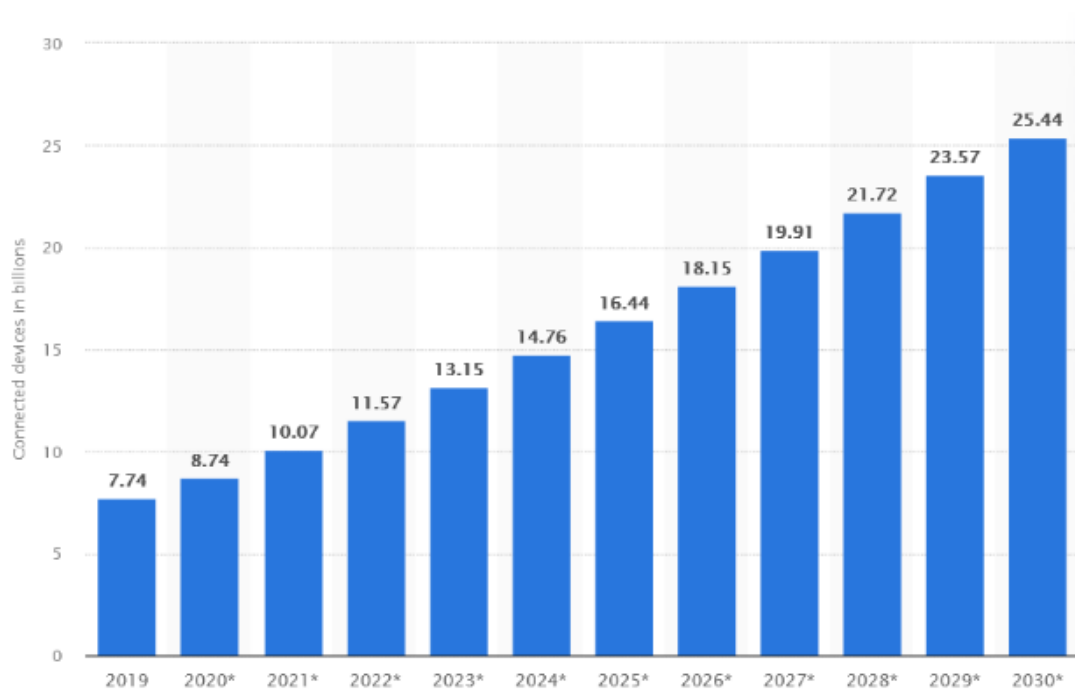


Figure 5. Connected IoT Devices 2019-2030 Forecast (Statista, 2022b).

Although OSINT offers many benefits, it also has shortcomings that should be acknowledged. One of its challenges is the abundance of gathered data that needs to be analysed and filtered, which is time-consuming. Multiple automation tools and artificial intelligence (AI) solutions are already available, but they still require active human involvement in reviewing and validating the results. Another issue is source credibility. Some media sources and even governments may publish misleading information for manipulation purposes. Before OSINT data can be trusted, it needs to be verified by classified sources or compared to data from reliable OSINT sources. (Hassan & Hijazi, 2018)

3.3 Resources, Tools, and Techniques

The Internet has several layers (Figure 6) and is a far greater data resource than most regular users are aware of. Cybercriminals have access to a wealth of data and tools hidden beyond search engine results. (Hassan & Hijazi, 2018)

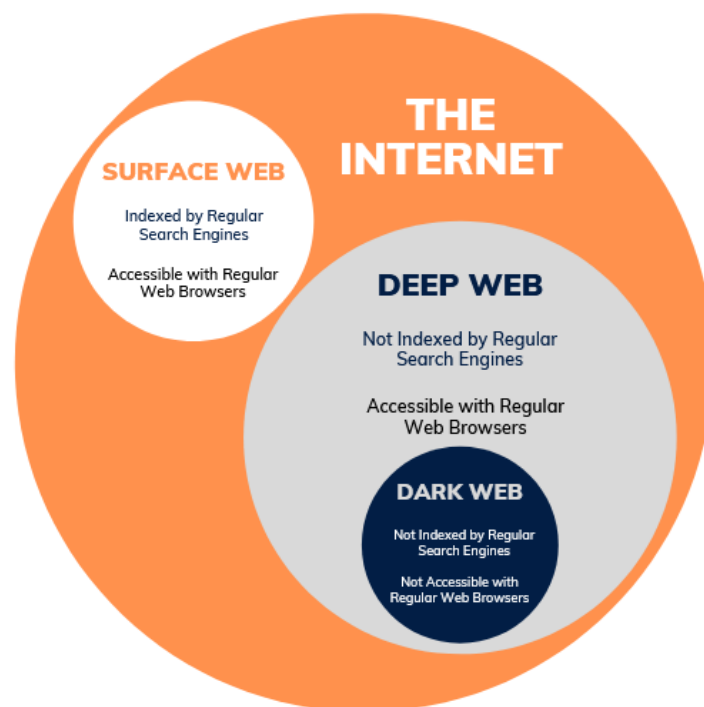


Figure 6. Layers of the Internet (Hassan & Hijazi, 2018).

The surface web is the internet layer that everyday users are familiar with, including websites and content that regular search engines have indexed in their databases. Essentially, it is content that can be found with a search query on Google, Bing, and other well-known search engines. The surface web is estimated to contain only 4% of all web content. The remaining 96% exists on the deep web, with content that cannot be found using regular search engines. Most deep web content is legitimate and can be accessed with a standard web browser using a direct web address (URL) or IP address. They are typically database content of surface web sources that may be openly accessible or require authorisation (e.g., cloud documents, unlisted YouTube videos, unlisted social media profiles, files uploaded on websites), public websites that want to stay hidden from standard searches on purpose, or private sources that require authorisation (e.g., government databases, medical records, and organisation databases). (Hassan & Hijazi, 2018)

The terms "deep web" and "dark web" are often used interchangeably, but the dark web is only a fraction of the deep web. It is impossible to measure the data on the dark web because of its unregulated nature, but a standard estimation is approximately 6% of total web content. The dark web is only accessible with specialised tools and configurations designed to hide online activities. Because of this, it is mainly known for its illegal marketplaces (e.g., drugs, weapons, human trafficking) and other serious criminal activities. However, legitimate content on the dark web exists and is provided by anonymity advocates, activists, independent news sources, and others. Many well-known websites are also available on the dark web, allowing users to remain anonymous or bypass government censorship. (Hassan & Hijazi, 2018)

There are numerous specialised search engines, tools, methods, and resources for discovering the deep web's hidden content. It is impossible and possibly unethical to list them all. However, the following list presents some techniques and web-based tools often used in OSINT investigations. Standalone programs and illicit methods are excluded. For privacy reasons, some details in the figures have been redacted.

OSINT Framework

The OSINT Framework (osintframework.com) is a dynamic website that contains a comprehensive set of OSINT tools and resources. It is one of the essential tools for OSINT investigation. Figure 7 displays a fraction of the framework.

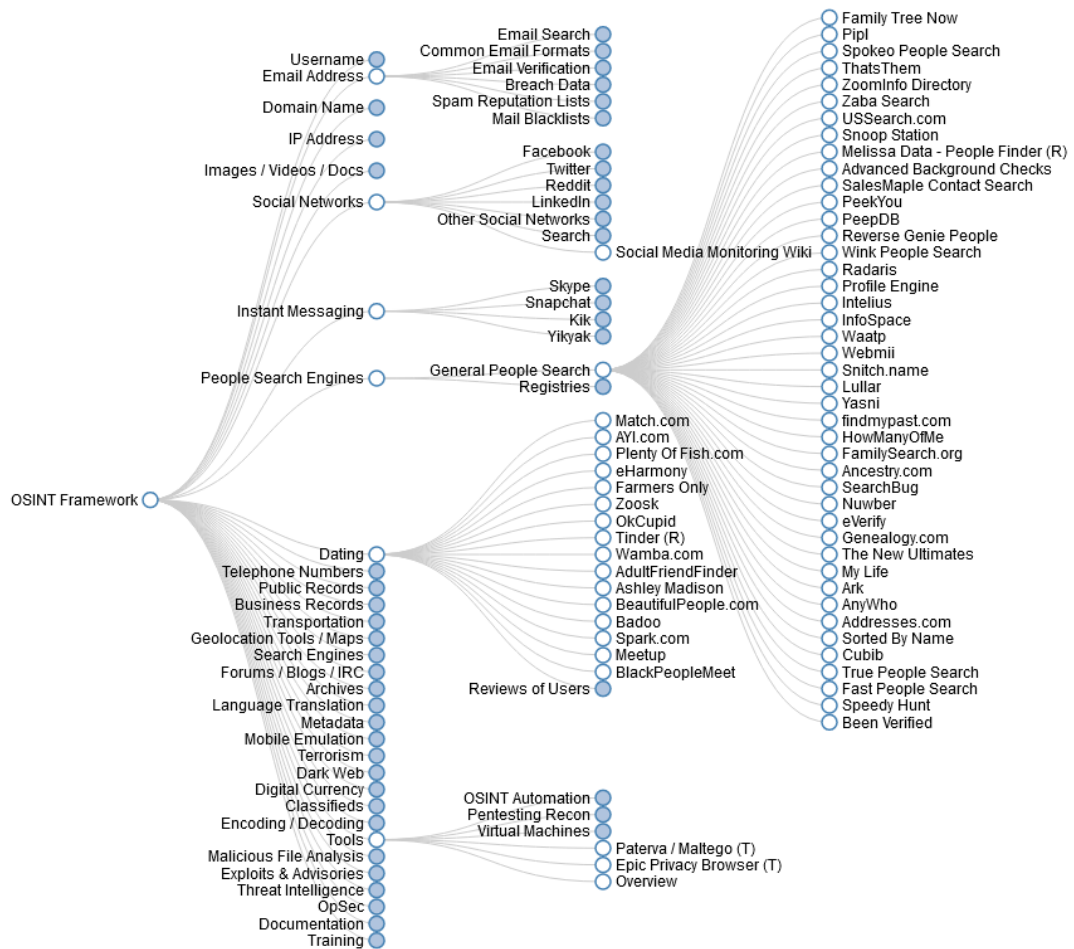


Figure 7. A Fraction of the OSINT Framework. (Nordine, n.d.)

Google Dorks and Advanced Search

Google advanced search ([google.com/advanced_search](https://www.google.com/advanced_search)) is an excellent tool for limiting search results, but it can also be a powerful method for discovering valuable information. The address bar on standard Google or any other website is just a command-based tool for requesting information from a database. Google "dorking" is the more versatile utilisation of search queries directly in the standard search bar. Search commands include basic Boolean operators (AND, OR), website-specific queries, and universal queries that work on numerous websites. This may be used to find content with specified attributes and filter out the rest. For instance, the search query "**filetype:pdf intitle:"social engineering" intext:OSINT | intext:intelligence**" (Figure 8) would search for only PDF files with the exact term "social engineering" in the title and mention of OSINT or intelligence in the text.

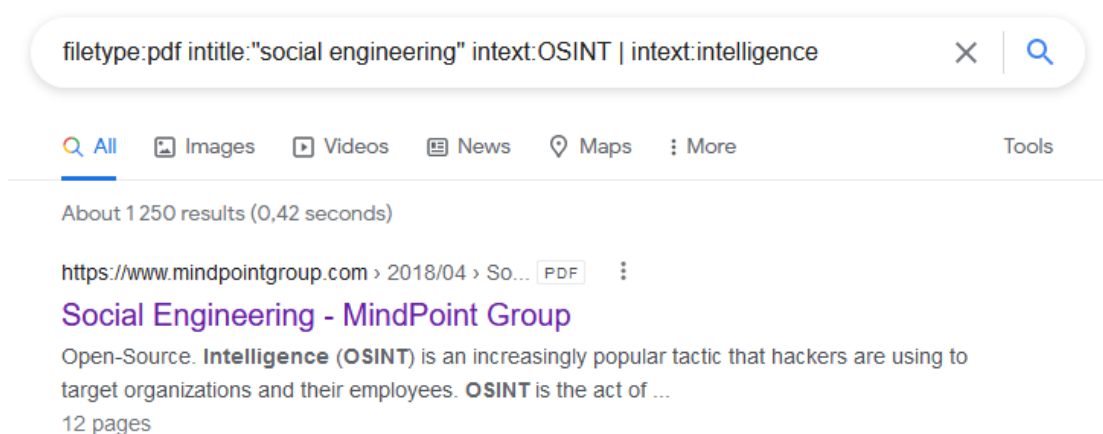


Figure 8. Google Dorking.

Cybercriminals can be highly creative with dorks by coming up with various combinations. They can discover confidential information from websites and servers that are not adequately secured. Table 1 lists some common "dorks."

Table 1. Popular Google Commands and Operators.

site:	Show only results from this website. Example: <i>site:amazon.com</i>
related:	Find similar websites. Example: <i>related:spotify.com</i>
filetype:	Find files with this extension. Example: <i>filetype:txt</i>
intitle:	Show results with this term in the title. Example: <i>intitle:101</i>
allintitle:	Show results with all these terms in the title. Example: <i>allintitle:zelda breath of the wild</i>
inurl:	Show results with this term in the URL. Example: <i>inurl:contact</i>
allinurl:	Show results with all these terms in the URL. Example: <i>allinurl:samsung galaxy</i>
intext:	Show results with this term in the text. Example: <i>intext:conclusion</i>
allintext:	Show results with all these terms in the text. Example: <i>allintext:tesla bmw audi</i>
OR 	Show results with one of these terms. Example: <i>film movie</i>
AND	Show only results with both terms. Example: <i>cats AND dogs</i>
-	Excludes results with this term. Example: <i>apple -iphone</i>
" "	Show only results with this exact phrase. Example: <i>"nikola tesla"</i>

Shodan

Shodan (*shodan.io*) is a search engine for internet-connected devices instead of websites. It can search for routers, servers, IoT devices (e.g., smart home gadgets, smartwatches, security cameras, and industrial systems), webcams, and so on. Shodan can discover and provide detailed information about any online device or system. If devices are not adequately secured, cybercriminals can use the information to exploit them with little effort. Figure 9 presents search results for webcams in Finland.

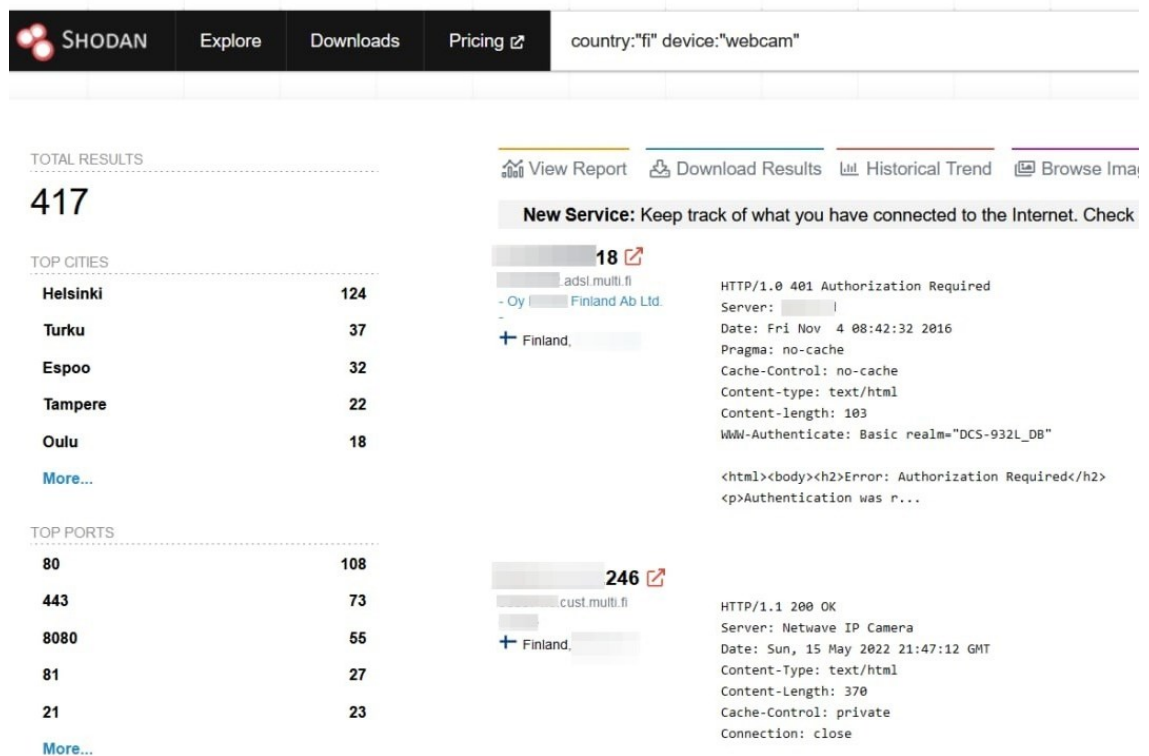


Figure 9. Shodan Search.

Social Media Platforms

Facebook previously had a robust hidden search function called "Graph Search," but it is no longer operational; nonetheless, its search filters are currently quite extensive. Popular social media platforms frequently change, making it difficult to keep track of the most recent social media intelligence (SOCMINT) developments. However, most public information is often readily accessible on social media profiles (e.g., friends, hobbies, location check-ins, images, posts). This information can then be used in the other OSINT tools to discover other accounts and details. The following tools can provide user account analytics or refine searches based on content, time, keywords, location, and other factors.

- Facebook advanced search: ***whopostedwhat.com***
- Twitter advanced search: ***twitter.com/search-advanced***
- Twitter analytics: ***socialbearing.com***
- Snapchat posts on a map: ***map.snapchat.com***
- Flickr photos on a map: ***flickr.com/map***
- Social media hashtag search: ***hashatit.com***

Webmii

Webmii (*webmii.com*) is a search engine that combines surface web information by automatically searching across multiple social media platforms and websites. Essentially, Google search results are displayed in a "profile" that lists the target's social network accounts, online article references, and acquaintances. Webmii is accurate when the target has a unique name, but it will combine the results of everyone with the same name.

The Internet Archive/The Wayback Machine

The Internet Archive (*archive.org*) is an online resource that offers free digital content to the public (Figure 10). This includes digitised analogue content, such

as book and document scans, VHS tapes, and microfilms. As part of the archive, The Wayback Machine (Figure 11) keeps website captures, including no longer operational sites. The archive currently holds over 35 million books and texts, over 682 billion websites, 7.9 million videos and movies, 842 thousand software applications, and 14 million audio files. (Wikipedia, 2022)

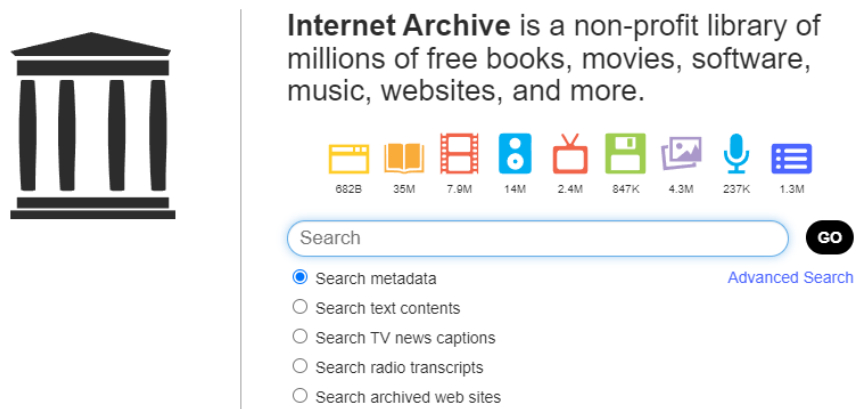


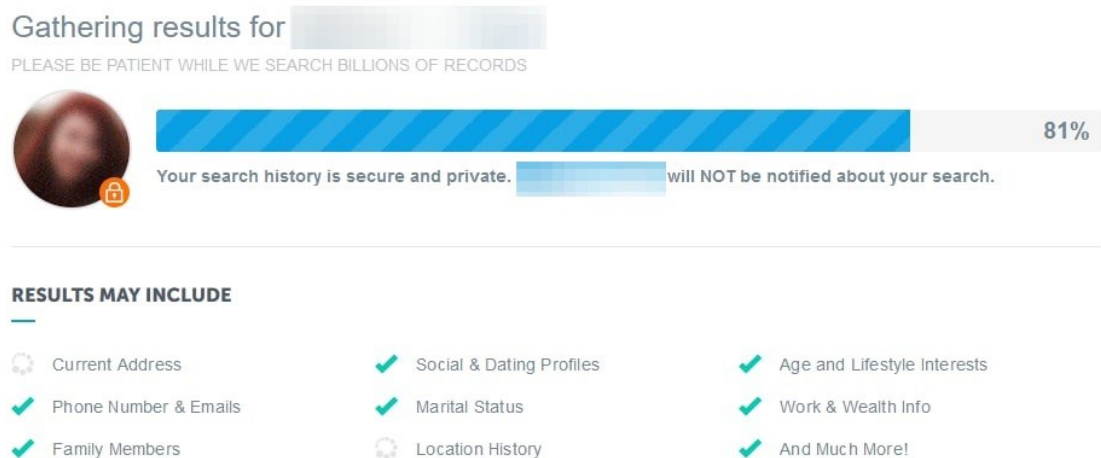
Figure 10. The Internet Archive.



Figure 11. The Wayback Machine Search.

Pipl/PeekYou/Spokeo

Pipl (*pipl.com*) is perhaps the most comprehensive people search engine. It can fetch information from searchable databases and deep web sources that are not indexed by standard search engines. Pipl is entirely commercial, so Spokeo (*spokeo.com*) and PeekYou (*peekyou.com*) are popular alternatives that offer some free information. They can return results based on someone's full name (Figure 12), email, phone number, username (Figure 13), or address.



Gathering results for [redacted]

PLEASE BE PATIENT WHILE WE SEARCH BILLIONS OF RECORDS

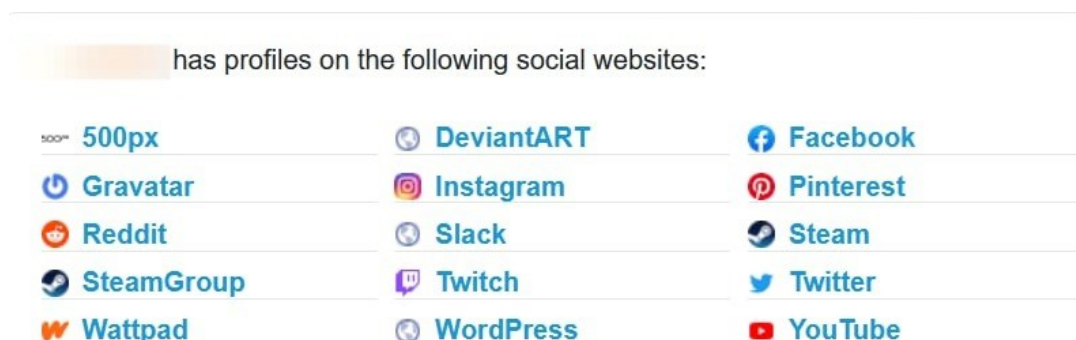
81%

Your search history is secure and private. [redacted] will NOT be notified about your search.

RESULTS MAY INCLUDE

- Current Address
- Phone Number & Emails
- Family Members
- Social & Dating Profiles
- Marital Status
- Location History
- Age and Lifestyle Interests
- Work & Wealth Info
- And Much More!

Figure 12. Spokeo Name Search.



[redacted] has profiles on the following social websites:

- 500px
- DeviantART
- Facebook
- Gravatar
- Instagram
- Pinterest
- Reddit
- Slack
- Steam
- SteamGroup
- Twitch
- Twitter
- Wattpad
- WordPress
- YouTube

Figure 13. PeekYou Username Search Results.

Have I Been Pwned?



Have I Been Pwned? (*haveibeenpwned.com*) is a service that gathers data dumps containing information on billions of user accounts that have been compromised in data breaches (Figure 14). Users can look up their data by entering their username or email address. It is an excellent method for checking if one's personal data has been leaked and signing up for future alerts. However, nothing prevents malicious actors from entering the target's details to find the leaked information in the paste files. They can contain usernames, emails, and passwords that often have not been changed yet because the target is unaware of the breach.

Oh no — pwned!

Pwned in 11 data breaches and found 3 pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Bitcoin Security Forum Gmail Dump: In September 2014, a large dump of nearly 5M usernames and passwords was posted to a Russian Bitcoin forum. Whilst commonly reported as 5M "Gmail passwords", the dump also contained 123k yandex.ru addresses. Whilst the origin of the breach remains unclear, the breached credentials were confirmed by multiple source as correct, albeit a number of years old.

Compromised data: Email addresses, Passwords

Pastes you were found in

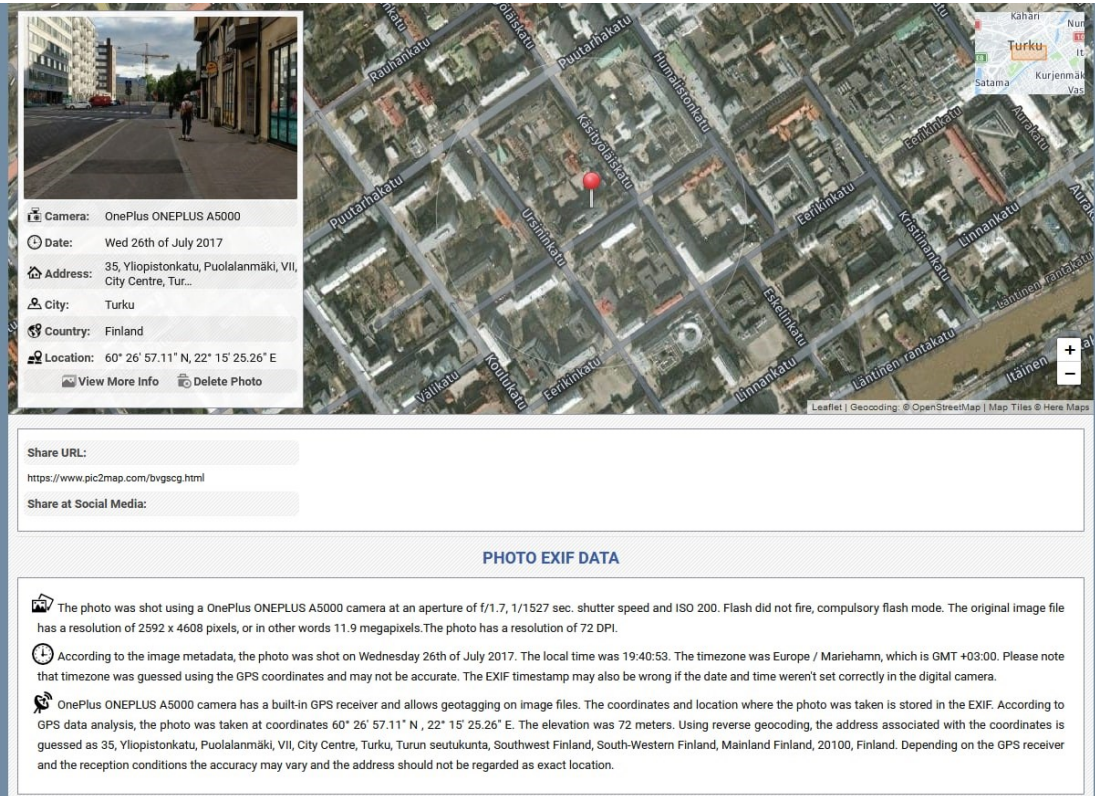
A paste is information that has been published to a publicly facing website designed to share content and is often an early indicator of a data breach. Pastes are automatically imported and often removed shortly after having been posted. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Paste title	Date	Emails
pred.me	Unknown	4,788,657
xn-e1alhsoq4c.xn-p1ai	Unknown	4,788,657
files.miyako.rocks	Unknown	975,853

Figure 14. Have I Been Pwned Results.

Pics2Map

Pic2Map (pic2map.com) is an EXIF data reader with GPS functionality that shows photo locations on Google Maps. EXIF is a file format for metadata about a digital photo or video. Most of the data is technical, such as camera and photo settings. Digital cameras also save date and time data. Location is often stored by default with smartphone cameras and cameras with internet connectivity, but it can be disabled manually. Pic2Map can pinpoint where the photo was taken (Figure 15), which is especially useful for malicious actors if the photo was taken at their target's address.



The screenshot displays the Pic2Map interface. On the left, a photo thumbnail is shown. Below it, the EXIF data is listed:

- Camera: OnePlus ONEPLUS A5000
- Date: Wed 26th of July 2017
- Address: 35, Yliopistonkatu, Puolalanmäki, VII, City Centre, Turku
- City: Turku
- Country: Finland
- Location: 60° 26' 57.11" N, 22° 15' 25.26" E

Below the photo and map, there is a "Share URL" field with the URL <https://www.pic2map.com/bvgsqj.html> and a "Share at Social Media" button. The "PHOTO EXIF DATA" section provides detailed technical information:

- The photo was shot using a OnePlus ONEPLUS A5000 camera at an aperture of $f/1.7$, $1/1527$ sec. shutter speed and ISO 200. Flash did not fire, compulsory flash mode. The original image file has a resolution of 2592 x 4608 pixels, or in other words 11.9 megapixels. The photo has a resolution of 72 DPI.
- According to the image metadata, the photo was shot on Wednesday 26th of July 2017. The local time was 19:40:53. The timezone was Europe / Mariehamn, which is GMT +03:00. Please note that timezone was guessed using the GPS coordinates and may not be accurate. The EXIF timestamp may also be wrong if the date and time weren't set correctly in the digital camera.
- OnePlus ONEPLUS A5000 camera has a built-in GPS receiver and allows geotagging on image files. The coordinates and location where the photo was taken is stored in the EXIF. According to GPS data analysis, the photo was taken at coordinates 60° 26' 57.11" N, 22° 15' 25.26" E. The elevation was 72 meters. Using reverse geocoding, the address associated with the coordinates is guessed as 35, Yliopistonkatu, Puolalanmäki, VII, City Centre, Turku, Turun seutukunta, Southwest Finland, South-Western Finland, Mainland Finland, 20100, Finland. Depending on the GPS receiver and the reception conditions the accuracy may vary and the address should not be regarded as exact location.

Figure 15. Pics2Map EXIF Extraction.

Hunter

Hunter (*hunter.io*) is an email address finder tool that searches the web for email formats and addresses (Figure 16) used by organisations. It is a useful tool for finding correct addresses for business contacts, but cybercriminals can use it to find addresses for phishing emails or use them for impersonation.

The screenshot shows the Hunter.io search interface. At the top, there is a search bar containing 'turkuamk.fi' and a red button labeled 'Find email addresses'. Below the search bar, the results are displayed as follows:

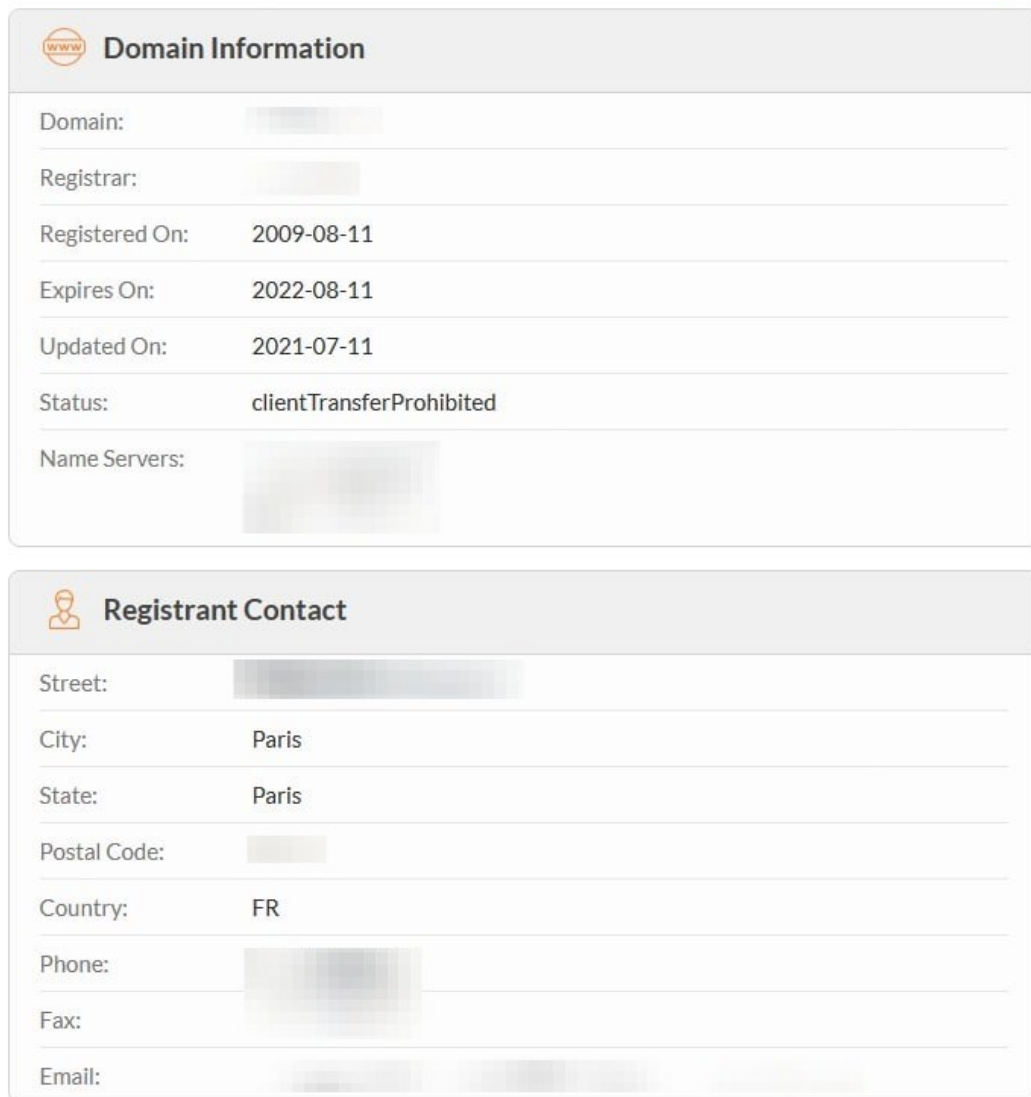
- Most common pattern: {first}.{last}@turkuamk.fi (531 email addresses)
- Result 1: [redacted]@turkuamk.fi (1 source)
- Result 2: [redacted]@turkuamk.fi (2 sources)
 - Source 1: <http://talk.turkuamk.fi/blog>, 2022
 - Source 2: <http://talk.turkuamk.fi/yrittajyys/>, Jul 21,
- Result 3: [redacted]@turkuamk.fi (5 sources)
- Result 4: [redacted]@turkuamk.fi (15 sources)
- Result 5: [redacted]@turkuamk.fi (6 sources)

At the bottom, it indicates '526 more results for turkuamk.fi.'

Figure 16. Hunter Search.

Whois

Whois (*whois.com/whois*) is a domain name and IP address lookup service. When a domain name is registered, the domain registration information is made public (Figure 17). The Whois database can search hundreds of domain registries for information such as registration date, expiration date, ownership, and contact information.



The image shows two sections of a Whois lookup result. The first section, titled 'Domain Information', contains the following data: Domain (blurred), Registrar (blurred), Registered On: 2009-08-11, Expires On: 2022-08-11, Updated On: 2021-07-11, Status: clientTransferProhibited, and Name Servers (blurred). The second section, titled 'Registrant Contact', contains: Street (blurred), City: Paris, State: Paris, Postal Code (blurred), Country: FR, Phone (blurred), Fax (blurred), and Email (blurred).

Domain Information	
Domain:	[blurred]
Registrar:	[blurred]
Registered On:	2009-08-11
Expires On:	2022-08-11
Updated On:	2021-07-11
Status:	clientTransferProhibited
Name Servers:	[blurred]

Registrant Contact	
Street:	[blurred]
City:	Paris
State:	Paris
Postal Code:	[blurred]
Country:	FR
Phone:	[blurred]
Fax:	[blurred]
Email:	[blurred]

Figure 17. Whois Domain Information.

4 Notable Incidents

RSA SecurID Data Breach (2011)

In March 2011, RSA Security, the network security firm best known for its SecurID two-factor authentication (2FA) devices, suffered a data breach. Phishing emails pretending to be from a job recruitment website were sent to four employees, including an Excel file. When the spreadsheet was opened, a zero-day Flash Player exploit hidden in it installed backdoor access to RSA's systems, compromising their data. RSA initially said that attackers would require more than the data they obtained to access client systems. Still, months later, hackers were detected attempting to access customer networks using cloned SecurID tokens. RSA ended up spending over \$66 million on the recovery and replacement of tokens. Not even security companies are immune to basic social engineering approaches. (Constantin, 2011)

Democratic National Committee Email Leak (2016)

The Democratic National Convention (DNC) email dumps were among the most noteworthy parts of the 2016 US presidential election, with over 150 000 stolen from more than a dozen Democrats and shared on Wikileaks and DCLeaks. Russian hackers sent phishing emails to DNC staff members that appeared to be from Google, warning them of strange activities on their email accounts and urging them to click on a link to reset their password. The website was likewise designed to look like Google, and the targets were told to enter their credentials. Once the attackers had the credentials, they gained access to private contact lists and thousands of emails containing sensitive information about the Clinton campaign. (Satter et al., 2017)

Facebook and Google Invoice Scam (2013-2015)

A Lithuanian con artist, Evaldas Rimasauskas, and his team impersonated Quanta Computer, a Taiwanese manufacturer previously working with Google and Facebook. They set up a bogus company with the same name and opened several bank accounts worldwide. Spear phishing emails containing forged invoices and contracts were sent to selected Google and Facebook employees. The invoices were for products and services supplied by the actual manufacturer, but payments were directed into the fraudulent accounts. The tech giants had paid Rimasauskas and his accomplices more than \$120 million between 2013 and 2015. (Romo, 2019)

Ukraine Power Grid Outage (2015)

Ukraine's power grid network was breached by Russian hackers months before the December 2015 power outage that affected around 225 000 consumers. After gaining access using a spear phishing email containing "BlackEnergy 3" malware in an Excel file, the attackers gathered intelligence and planned their main attack for months before exploiting the network-connected control systems. Although numerous other Ukrainian and global energy facilities have since suffered a variety of cyberattacks, this was the first successful case that resulted in a blackout. (Harrell, 2017)

Twitter Hijacked Accounts Bitcoin Scam (2020)

Around 130 official Twitter accounts of influential individuals and businesses were taken over and used in a Bitcoin hoax in July 2020. Among them were Barack Obama, Elon Musk, Bill Gates, Jeff Bezos, Kanye West, Apple, and Uber. Attackers gained access to the accounts through a phone spear phishing attack that targeted Twitter employees with administrative access, then utilised it to make posts (Figure 18) that tricked users into sending them Bitcoins in the hopes

of doubling the money. More than 320 transactions took place just minutes after the first posts, sending over \$110 000 worth of Bitcoins to one address before Twitter deleted them. (BBC News, 2020; Twitter, 2020)



Figure 18. Twitter Bitcoin Scam.

Yahoo Data Breach (2013)

The Yahoo! 2013 data breach was initially reported to have affected 500 million users, but it was later revealed in 2017 that it had affected all three billion users. The attackers gained access to Yahoo's systems and the complete user database with spear phishing emails containing malicious hyperlinks. Stolen data, including full names and passwords, was sold on the dark web and most likely used in additional attacks on users. This remains the largest data breach in history, and the hacker's identity responsible for it remains unknown. Since then, Yahoo! has faced numerous other data breaches and was purchased by Verizon in 2017. (Newman, 2017; Weinreb, 2019)

Vastaamo Data Breach (2018-2020)

The Finnish psychotherapy centre, Vastaamo, announced in October 2020 that they had suffered a data breach. Attackers stole approximately 40 000 patient records and demanded a ransom of forty Bitcoins (equal to €450 000 at the time) for not leaking the data on the dark web (Figure 19). It was not a ransomware attack because the data was still accessible, but the confidential nature of the information allowed for extortion. When Vastaamo refused to pay the ransom, the attackers attempted to extort the patients directly. Although some data was leaked, the threat to release everything after the deadline was not followed through. It is still uncertain whether anyone paid the ransom. Data breach victims have filed over 25,000 criminal reports. (Waldman, 2020)



Figure 19. Vastaamo Ransom Message (Aves Netsec, 2020).

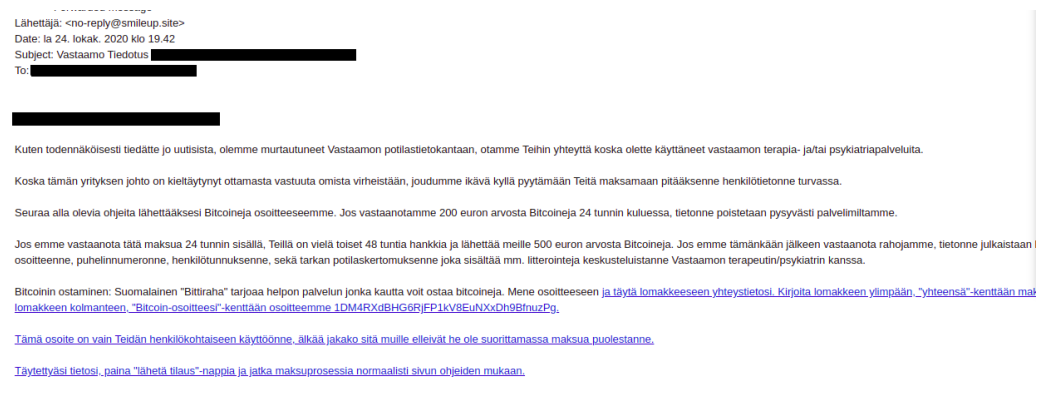


Figure 20. Vastaamo Patient Ransom Message (Aves Netsec, 2020).

5 Countermeasures

Social engineering attacks are among the most difficult to defend against. However, individuals and organisations may significantly reduce the risks by exercising a few precautions. Prevention is the most effective defence, and security awareness training is the most effective means of prevention. Adopting the proper mindset will assist in tackling emerging threats, even when little is still known about them. A list of suggested social engineering countermeasures is provided below. (CompTIA, n.d.)

5.1 Individuals

- Be cautious of emails, texts, and calls from unknown individuals.
- Look up unfamiliar email addresses and phone numbers on the web.
- If you receive a strange email from someone you know, double-check their email address and contact them through other methods to confirm.
- Always use two-factor authentication on services that support it.
- Before clicking on hyperlinks or attachments, verify that the sender is who they claim to be.
- Do not publish personal details on social media. Set your profile to private and validate friend and follow requests. Avoid using the same username on every platform.
- Do not enter your credentials if a hyperlink takes you to a website that demands you to log in to see the contents or change your password.
- Do not comply with emails, texts, or calls requesting passwords, bank information, or other sensitive information.
- Do not react to urgent pleas from unknown individuals.
- Do not open any emails that promise rewards.
- Do not be alarmed if a pop-up claims your system is infected, and do not click on it. Use malware/virus protection software downloaded from a trusted source to scan the system. (CompTIA, n.d.)

- Visit haveibeenpwnd.com to check whether your accounts were compromised in a data breach. If this is the case, you should change your passwords **on all services that utilise the same credentials**.
- Avoid using easily guessable or short passwords. Combine lowercase and capital letters, digits, and symbols. Never reveal or hint at your password to anybody. Do not use the same password everywhere, especially for services that have access to payment methods. More details on password security and a password strength test tool can be found at security.org/how-secure-is-my-password.

5.2 Organisations

- Security protocols and methods should be taught to all levels of personnel. Increase social engineering awareness within the organisation. Reinforce training with random simulation testing.
- Access to sensitive information should be limited. Establish proper access privileges. There should be different authorisation levels depending on the role. (ICT Byte, 2022)

5.3 Phishing Warning Signs

- Appears to be from someone familiar, but the address does not match.
- Contains an unexpected or strange attachment.
- Appear to be urgent or contains a subtle warning.
- Contains hyperlinks that look strange or disguised.
- Appears to be a poor translation or has strange grammatical errors.
- Contains a generic message and appears to be from a genuine firm.
- Contains unlikely proposals, prizes, or bargains. (ICT Byte, 2022)

6 Conclusions

In recent years, I have been increasingly interested in online privacy, primarily in the context of web surveillance and data gathering practised by businesses and governments. As this issue has become more widely discussed, many have stated that they are not bothered by it because they have nothing to hide; that internet surveillance is a positive thing since it helps catch criminals; and that only people participating in suspicious activities should be concerned. However, the study's findings revealed that it is about far more than the right to privacy and putting a stop to "Big Brother". The value of personal data extends far beyond web surveillance, "free" services in return, and targeted marketing.

I became interested in social engineering concepts while watching one of my favourite television series, Mr Robot. After some exploration, I realised that some of my other favourite works featured a wide range of social engineering elements. Everyone has seen these techniques in action, whether in fiction or real life, yet most are unaware of their widespread usage in cyberattacks.

With the ongoing pandemic and war, the current relevancy of social engineering and open-source intelligence is undeniable. Information has always been one of the most valuable assets, but now it is more abundant, easier to access and more creatively exploited. The intent of this review was not to make people feel anxious about potential threats but rather to promote awareness and encourage individuals and organisations to take prevention measures, so cybercriminals would find it more challenging to succeed.

The main takeaway is that, regardless of how many think they would never fall for these exploits that have deceived others, the human mind will always be more exploitable than modern technology. Data breaches at leading technology and security firms demonstrate this. Anyone can fall victim to social engineering if they are unaware of these manipulative methods. Another impressive and unpredictable element is creativity. There are far more approaches and tools than what was covered, and new ones are constantly emerging, so training and adopting a proper mindset is critical for defending against future threats.

References

- Aves Netsec. (2020). *Psychotherapy Clinic Chain is Having Their Patients Directly Ransomed*. Aves Netsec.
<https://www.avesnetsec.com/psychotherapy-ransom>
- Bazzell, M. (2022). *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*. Self-Published.
- BBC News. (2020). *Major US Twitter Accounts Hacked in Bitcoin Scam*. BBC News. <https://www.bbc.com/news/technology-53425822>
- Beffa, E. (2020). *What is OSINT? Open Source Intelligence in the Legal Field*. Colorado Lawyer. <https://cl.cobar.org/departments/what-is-osint/>
- Buxton, O. (2021). *What Is Scareware? Detection, Prevention & Removal*. Avast. <https://www.avast.com/c-scareware>
- Cialdini, R. B. (2021). *Influence: The Psychology of Persuasion*. Harper Business.
- Cisco. (2021). *2021 Cyber Security Threat Trends - Phishing, Crypto Top the List*. <https://learn-umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list>
- CompTIA. (n.d.). *What Is Social Engineering? The Human Element in the Technology Scam*. CompTIA. Retrieved March 16, 2022, from <https://www.comptia.org/content/articles/what-is-social-engineering>
- Constantin, L. (2011). *SecurID Data Breach Cost RSA \$66 Million*. Softpedia News. <https://news.softpedia.com/news/SecurID-Data-Breach-Costs-RSA-66-Million-214318.shtml>
- CrowdStrike. (2022). *Open Source Intelligence (OSINT)*. CrowdStrike. <https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/>
- ENISA. (n.d.). *What is Social Engineering?* ENISA. Retrieved May 3, 2022, from <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering>

- Galov, N. (2022). *17+ Sinister Social Engineering Statistics for 2022*. Web Tribunal. <https://webtribunal.net/blog/social-engineering-statistics/>
- GOV.UK. (2022). *Cyber Security Breaches Survey 2022*. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022>
- Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. John Wiley & Sons Inc.
- Harrell, B. (2017). *Why the Ukraine Power Grid Attacks Should Raise Alarm*. CSO. <https://www.csoonline.com/article/3177209/why-the-ukraine-power-grid-attacks-should-raise-alarm.html>
- Hassan, N. A., & Hijazi, R. (2018). *Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence*. Apress.
- ICT Byte. (2022). *Social Engineering Explained in Simple Way*. ICT Byte. <https://ictbyte.com/masters-of-computer-science/social-engineering-explained-in-simple-way>
- Malwarebytes. (n.d.). *What is Phishing?* Malwarebytes. Retrieved April 1, 2022, from <https://www.malwarebytes.com/phishing>
- Mitnick Security. (n.d.). *The History of Social Engineering & How to Stay Safe Today*. Mitnick Security. Retrieved March 25, 2022, from <https://www.mitnicksecurity.com/the-history-of-social-engineering>
- National Cyber Security Centre. (2018). *Phishing Attacks: Defending Your Organisation*. NCSC.GOV.UK. <https://www.ncsc.gov.uk/guidance/phishing>
- Newman, L. H. (2017). *Yahoo's 2013 Email Hack Actually Compromised Three Billion Accounts*. WIRED. <https://www.wired.com/story/yahoo-breach-three-billion-accounts/>
- Nordine, J. (n.d.). *OSINT Framework*. OSINT Framework. Retrieved March 1, 2022, from <https://osintframework.com/>
- Panda Security. (2021). *11 Types of Phishing + Real-Life Examples*. Panda Security. <https://www.pandasecurity.com/en/mediacenter/tips/types-of-phishing/>

Pilette, C. (2021). *What is Social Engineering? A Definition + Techniques to Watch for*. Norton. <https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html>

Police Act, Pub. L. No. 872/2011, Ministry of the Interior, Finland (2011). https://www.finlex.fi/en/laki/kaannokset/2011/en20110872_20131168.pdf

Romo, V. (2019). *Man Pleads Guilty to Phishing Scheme That Fleeced Facebook, Google of \$100 Million*. NPR. <https://www.npr.org/2019/03/25/706715377/man-pleads-guilty-to-phishing-scheme-that-fleeced-facebook-google-of-100-million>

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. In *Future Internet*. MDPI AG. <https://doi.org/10.3390/FI11040089>

Satter, R. (2020). *US Court: Mass Surveillance Program Exposed by Snowden Was Illegal*. Reuters. <https://www.reuters.com/article/us-usa-nsa-spying-idUSKBN25T3CK>

Satter, R., Donn, J., & Day, C. (2017). *Inside Story: How Russians Hacked the Democrats' Emails*. AP News. <https://apnews.com/article/technology-europe-russia-hacking-only-on-ap-dea73efc01594839957c3c9a6c962b8a>

Statista. (2022a). *Internet Users in the World 2022*. Statista. <https://www.statista.com/statistics/617136/digital-population-worldwide/>

Statista. (2022b). *IoT Connected Devices Worldwide 2019-2030*. Statista. <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>

Suojelupoliisi. (n.d.). *Intelligence Gathering Seeks Unique Information*. Finnish Security and Intelligence Service. Retrieved March 7, 2022, from <https://supo.fi/en/intelligence-gathering>

Talamantes, J. (2014). *The Social Engineer's Playbook: A Practical Guide to Pretexting*. Hexcode Publishing. <https://www.redteamsecure.com/research/the-social-engineers-playbook-a-practical-guide-to-pretexting>

The Associated Press. (2020). *The Latest: UN Warns Cybercrime on Rise During Pandemic*. ABC News.

<https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542>

Twitter. (2020). *An Update on Our Security Incident*. Twitter Blog. https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident

Waldman, A. (2020). *25,000 Criminal Reports: Vastaamo Breach Sets New Precedent*. Tech Target.

<https://www.techtarget.com/searchsecurity/news/252492019/25000-criminal-reports-Vastaamo-breach-sets-new-precedent>

Weinreb, D. (2019). *How Did the Yahoo Data Breach Happen?* Dan Wein Reb. <https://www.danweinreb.org/breaching-billions-a-look-into-the-yahoo-data-breach/>

Wikipedia. (2022). *Internet Archive*. Wikipedia. https://en.wikipedia.org/wiki/Internet_Archive

Zarembo, K., & Solodkyy, S. (2021). *The Evolution of Russian Hybrid Warfare: Ukraine*. CEPA. <https://cepa.org/the-evolution-of-russian-hybrid-warfare-ukraine/>