



From January 2019 to April 2020

# Identity theft

ENISA Threat Landscape



# Overview

Identity theft or identify fraud is the illicit use of a victim's personal identifiable information (PII) by an impostor to impersonate that person and gain a financial advantage and other benefits.

According to an annual security report, at least 900 international cases of identity theft or identity-related crimes were detected<sup>1</sup>. The most significant incidents reported were:

- the exposure of nearly 106 million American and Canadian bank customers' personal information from the Capital One data breach incident in March 2019<sup>2</sup>;
- the exposure of 170 million usernames and passwords used by digital game developer Zynga in September 2019;
- the stealing of 20 million accounts from the British audio streaming service Mixcloud<sup>3</sup>;
- the compromise of 600,000 drivers and 57 million users personal information from Uber's data breach incident in November 2019;<sup>3</sup>
- and the theft of 9 million personal records from EasyJet customers including identity cards and credit cards.

The trend of identity theft is reflected to a great part in data breaches, which, compared with 2018, saw a record number of 3.800 publicly disclosed cases, 4,1 billion records exposed and an increase of 54% in the number of breaches reported.<sup>4</sup>





## Findings

The average cost for credential theft

**\$493,093**

The annual cost for credential theft

**\$2,79M**

The frequency of incidents per company in 2019

**3.2**

Percentage of incidents relating to negligence

**63%**

Source: From a IBM Security Study – Cost of Insider Threats: Global Report<sup>13</sup>

## The identity theft threat

In 2019, some malicious actors behind major incidents from the past years were brought to justice. In June, the New York Police Department, in collaboration with the FBI, brought to justice the members of the 'Fraud Ring', who operated inside and outside the United States and managed in 2012 to steal credentials from iPhones worth of US \$1million (ca. €846.000) in a large-scale identity theft operation. Until the group was stopped, the total amount stolen reached US \$19 million (ca. €16 million)<sup>4</sup>. A month later, the 'Equifax settlement' was publicly announced<sup>5</sup>. Equifax was forced to agree to compensate the United States Federal Trade Commission, the Consumer Financial Protection Bureau, 48 states, District of Columbia and Puerto Rico over its 2017 data breach at the cost of at least US \$575 million (ca. €487 million). Because of that data breach, which was ruled as 'entirely preventable', nearly 148 million American addresses and social security numbers were leaked. At the end of the year, Brazil fined Facebook in US \$1,6 million (ca. €1,35 million) on behalf of Brazilian citizens for the Cambridge Analytica data leak.<sup>3</sup>

# Kill chain


## Identity theft

Reconnaissance

Weaponisation

Delivery

Exploitation

 *Step of Attack Workflow*

 *Width of Purpose*



The Cyber Kill Chain® framework was developed by Lockheed Martin, adapted from a military concept related with the structure of an attack. To study a particular attack vector, use this kill-chain diagram to map each step of the process and reference the tools, techniques and procedures used by the attacker.

[MORE INFORMATION](#)

## Brand impersonation attacks

Consistent with the trend in 2018, certain brands are preferred in impersonation attacks because of their strong reputation. Although these brands - such as Microsoft (44%) and Amazon (17%) - continue to lead in the rankings of 2019 brand impersonation attacks, new additions such as the United States Internal Revenue Service (IRS) are notable.<sup>7</sup> The sensitive information included in the Wage and Tax Statement (W-2) has always been appealing to impostors, who used an IRS impersonation in 10% of identity deception-based e-mails in this reporting year. As a result, valid W-2 forms and standard US Individual Tax Return (1040) forms are available on the dark web at a cost ranging between US \$1 and US \$52.

This material, combined with the Social Security Numbers (SSN) and birth dates, which are also available, allows any inexperienced hacker willing to invest an amount of US \$1,000 (ca. €846) to legally access a United States-based bank account, file a false tax return, claim a refund and cash-out an investment that has doubled or tripled. According to the IRS Criminal Investigation, more than 10.000 individual tax returns with claims for refund of more than US \$83 million (ca. €70 million) were potentially fraudulent.<sup>8</sup>

# The cycle of steps for the tax scam “Dirty Dozen”



Source: BDO<sup>19</sup>

## **\_SIM-Swapping identities**

This technique has been used since 2016, targeting cryptocurrency holders. However, in 2019 the same technique was used against high-profile individuals or accounts with the intention of stealing the victim's identity. A number of victims of SIM-swapping were recorded, such as Jack Dorsey (Twitter's CEO), Jessica Alba (actor), Shane Dawson (actor), Amanda Cerny (actor, twice a victim), Matthew Smith (actor, four times victim) and King Bach (artist).<sup>10</sup> SIM-swapping was also used massively in two cases; at Mozambique's largest bank, where up to US \$50.000 (ca. €42.300) were stolen from high profile business accounts, and in Brazil where 5.000 victims, mainly politicians, ministers and governors had their accounts hacked by an organized gang.<sup>11</sup>

## **\_Gift cards used as a business e-mail compromise (BEC) trojan horse**

BEC attacks caused losses of billions of euros in 2019. In such incidents, the attackers impersonate a trusted individual, usually within the company, and the victim is tricked into making a financial transaction or divulging sensitive information, personal or corporate. In more than half of BEC attacks, the victim was lured into purchasing a gift card. During the purchase process, sensitive information such as bank account credentials was intercepted. The victim was also forced to send the gift card to the attacker, as an anonymous, irreversible and direct cash-out option. The average amount stolen per gift card reached US \$1.500 (ca. €1.269).<sup>12</sup>





## Findings

**20%** of identity deception attacks used compromised accounts<sup>7</sup>

**30%** of the attacks targeting C-level executives accounts were compromised using display name deception<sup>7</sup>

**65%** of BEC attacks lured victims to purchase gift cards<sup>12</sup>

**€3,32\_** million average cost of a data breach

**95%** of the responders to a Eurobarometer survey saw identity theft as a serious crime



## Digital doppelgangers

The anti-fraud technique 'digital masks' was exposed when more than 60.000 stolen digital identities appeared as a trading product on the darknet marketplace Genesis in April 2019. These doppelgangers were readily available to purchase at US \$5 - \$200 each. The owner of a doppelganger can more easily mimic a real user in an online shop or payment service, especially if this is combined with stolen logins and passwords. Apart from purchasing digital doppelgangers, new tools to assist the potential impersonator have appeared, such as the Tenebris browser, which embeds a generator allowing the unique fingerprints and digital masks to be developed.<sup>11</sup>

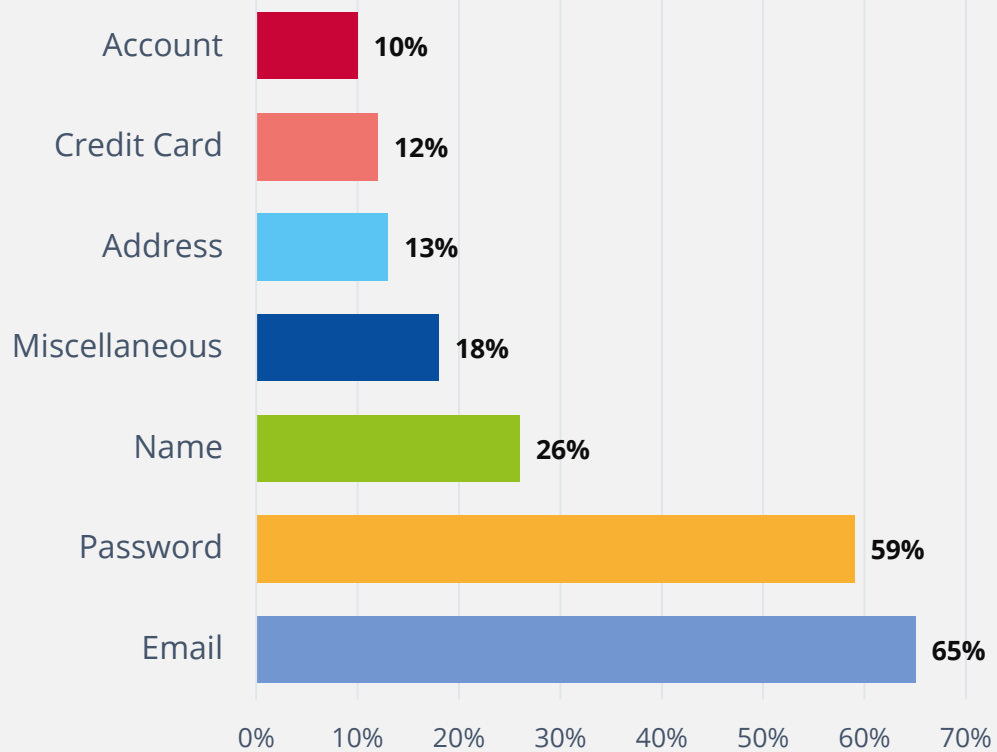
In recent years, skimmers, dumpster divers, hackers, administrator impersonators and phishers have been identified as the main groups behind the identity theft attacks. That list expanded in 2019 with the addition of vishers and smishers. Vishers phish via phone calls. Unlike telephone impersonators, vishers pretend to represent a well-known organisation and offer to assist the victim with a service, for example managing computer software, finances or a tax refund. Smishers send false SMS messages and, if the receiver replies, their device is directly hijacked or redirected to a phishing website.

The figure below shows the top data types lost in 2019, where e-mail data accounts for the highest number of records lost or stolen. These numbers reveals the seriousness of the situation when considering that e-mails may contain personal, corporate and governmental sensitive information.





## Top data types lost in 2019



Source: RiskBased SECURITY<sup>8</sup>

# Attack vectors

## How

- **THE CLOUD AS AN ATTACK INTERFACE FOR CUSTOMERS' DATA.** In the reporting year, Amazon CloudFront, a content delivery network (CDN), was compromised.<sup>14</sup> The websites hosted or linked to libraries on Amazon's infrastructure were exposed, revealing externally loaded content, including credit card data.
- **PHISHING URL.** The common malware URL techniques<sup>16</sup> of domain squatting, domain shadowing and URL shorteners were used once again in 2019. In the last quarter of 2019, it was noted that 26% of the malicious domains used a secure certificate and one in three of those certificates was SSL. This trick interfered with the judgement of visitor's who used to rely on the padlock icon in their browsers as a sign of security.<sup>15</sup>
- **W2 SCAM.** Another attack that targets companies and organisations' records to access sensitive information is the W2 scam. The scam starts by spoofing an executive member of the finance or human resources department to obtain employees' records. These records are then used for identity theft. The scam is named after the American W2 tax form used to report employee's wages. This social engineering scam, although old (first reported in 2016 by IRS), has been consistently rising by 10% every year in recent years.<sup>9,17</sup>
- **NIMCY.** In 2019, a spear-phishing tool, Nimcy was introduced by the group responsible for the Zebrocy malware family. It was developed using the Nim (formerly Nimrod) programming language, created by the same group of hackers. This new downloader and backdoor was used to steal login credentials, keystrokes, communications and files from diplomats, defence officials and ministry staff in the foreign affairs sector. The attackers seemed to focus on Central Asian governments, with a preference for Pakistan and India.<sup>14</sup>



- **MOBILE THREATS.** A rise in malicious mobile apps was noticed in 2019 and continued in 2020. Even widely used and trusted platforms such as Google Play were hosting apps aiming to steal credentials (e.g. Accesse SantaMobile, Modulo ID). However, the number of downloads was extremely low, showing that the potential victims were not fooled.<sup>20</sup>
- **TROJAN-BANKER.ANDROIDOS.SVPENG.AK** The eighth most popular mobile trojan and most popular mobile banking trojan, responsible for 1,75% and 16,85% of unique attacks respectively, mostly target victims' bank credentials and two-factor authorization codes. The majority of this trojan's victims are located in Russia, making it the top country in terms of share of users attacked by mobile banking trojans.<sup>21</sup>
- **FORMJACKING.** Formjacking was extremely common in 2018 but the number of attacks seemed to decrease considerably in the first quarter of 2019. However, starting in May with the attack on an American healthcare provider and the theft of login credentials, the number of attacks continued to rise throughout the rest of the year. In that month an all-time high number of 1,1 million detections was recorded. The five countries with the most formjacking detections in 2019 were the United States (51,8%), Australia (8,1%), India (5,7%), the United Kingdom (4,1%) and Brazil (3,5%). The Megacart hacker group is strongly associated with most of the development of formjacking tools and the attacks on British Airways, Newegg, Feedify and Ticketmaster<sup>22</sup>

## Proposed actions

- Avoid using the password manager provided by the browser. If one is needed, use an offline protected password manager.<sup>23</sup>
- Authenticate any sender of a request to transfer money by telephone or in person.<sup>19</sup>
- Do not share sensitive information such as patient records in handwritten notes to prevent their loss or misplacement. Digital files are better for data with a short lifetime and then they should be completely destroyed.
- Use 'threat hunting' within your company to strengthen security plans. Threat hunting is conducted by skilled members of the security operation centre (SOC) team to proactively identify vulnerabilities and prevent threats exploiting them.
- Use policies such as velocity-based rules to mitigate identity fraud, especially for payment card transactions. The machine data of valid transactions can provide sufficient information for optimal policy definition.
- Use single-sign-on (SSO) authentication method, when available, which allows a user to access several applications with the same set of digital credentials. Its use is highly recommended to minimise the number of user accounts and stored credentials.
- Install end-point protection by means of anti-virus programs but also block execution of files appropriately (e.g. block execution in the temp folder).
- Multi-factor authentication is a security measure to overcome password hacking or loss and to ensure the success of the authentication process with multiple keys. Introducing adaptive Multi-factor authentication optimise the authentication process based on the user's behaviour and on the associated context.



- Check URLs that are sent by e-mail or randomly visited based on their IP address, the ASN associated with the IP, the owner of the domain and the relation between this domain and others, before any further steps are taken.
- Organisations using cloud services should have strong cloud security operations and preferably use an architecture of on-premises storage, private cloud storage and public cloud storage simultaneously to protect their customer's personal information.
- Enforce the use of strong and updated encryption methods such as TLS 1.3 (using ephemeral keys) for sensitive data to prevent hacking.
- Adequately protect all identity documents and copies (physical or digital) against unauthorised access.
- Do not disclose identity information to unsolicited recipients and requests by phone or e-mail or in person should not be answered.
- Enforce the use of password protected devices, ensuring good quality of credentials, and secure methods for their storage.
- Ensure good quality of credentials and secure methods for their storage in all used media.
- Pay close attention when using public Wi-Fi networks, as fraudsters hack or mimic them. If one is used, avoid accessing sensitive applications and data. Use a trusted VPN service to connect to public Wi-Fi networks.
- Check transactions documented by bank statements or received receipts regularly for irregularities.
- Install content filtering to filter out unwanted attachments, mails with malicious content, spam and unwanted network traffic.
- Enforce the use of data loss prevention (DLP) solutions.

# References

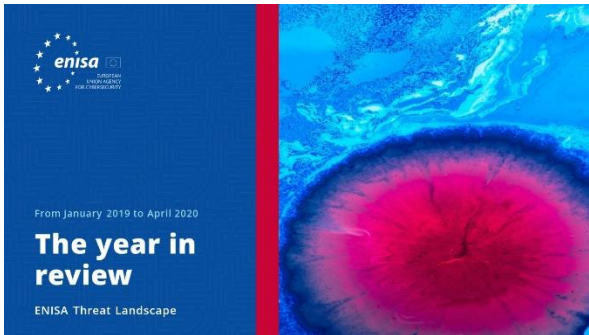
1. "2019 identity theft report released" July 31, 2019. ITIJ. <https://www.itij.com/latest/news/2019-identity-theft-report-released>
2. "Capital One data breach: What you can do now following bank hack" August 12, 2019. C|Net. <https://www.cnet.com/how-to/capital-one-data-breach-what-you-can-do-now-following-bank-hack/>
3. "Cybercrime Diary, Vol. 4, No. 4: Who's Hacked? Latest Data Breaches And Cyberattacks". January 8, 2020. Cyber crime Magazine. <https://cybersecurityventures.com/cybercrime-diary-q1-2020-whos-hacked-latest-data-breaches-and-cyberattacks/>
4. "\$19 million worth of iPhones stolen in massive identity theft scam" June 15, 2019. 9To5Mac. <https://9to5mac.com/2019/06/05/19-million-worth-of-iphones/>
5. "Equifax to pay at least \$575 million as part of FTC settlement " July 22, 2019. C|Net. <https://www.cnet.com/news/equifax-to-pay-at-least-575m-as-part-of-ftc-settlement/>
6. "2019 data breaches: 4 billion records breached so far" Norton. <https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html>
7. "Q1 2019: Email Fraud and Identity Deception Trends" Agari. <https://www.agari.com/insights/ebooks/2019-q1-report/>
8. "Data Breach QuickView Report, 2019 Q3 trends." November, 2019. RiskBased SECURITY. <https://pages.riskbasedsecurity.com/hubfs/Reports/2019/Data%20Breach%20QuickView%20Report%202019%20Q3%20Trends.pdf>
9. "IRS issues 2019 annual report; highlights program areas across the agency" January 6, 2020. IRS. <https://www.irs.gov/newsroom/irs-issues-2019-annual-report-highlights-program-areas-across-the-agency>
10. "Hackers Hit Twitter C.E.O. Jack Dorsey in a 'SIM Swap.' You're at Risk, Too" September 5, 2019. The New York Times. <https://www.nytimes.com/2019/09/05/technology/sim-swap-jack-dorsey-hack.html>
11. "IT threat evolution Q2 2019" August 19, 2019. Kaspersky. <https://securelist.com/it-threat-evolution-q2-2019/91994/>
12. "Phishing Activity Trends Report" September 12, 2019. Anti-phishing Working Group. [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q2\\_2019.pdf](https://docs.apwg.org/reports/apwg_trends_report_q2_2019.pdf)
13. "The Cost of Insider Threats" IBM. <https://www.ibm.com/downloads/cas/LQZ4RONE>
14. "APT trends report Q2 2019" August 1, 2019. Kaspersky. <https://securelist.com/apt-trends-report-q2-2019/91897/>
15. "Proof Point Q3 2019 threat report: Emotets return, rats reign supreme and more" Proof Point. <https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more>
16. ENISA Threat Landscape Report 2018. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>
17. "Q2 2019 Cryptocurrency Anti-Money Laundering Report" Cipher Trace. <https://ciphertrace.com/q2-2019-cryptocurrency-anti-money-laundering-report/>
18. "Latest Quarterly Threat Report - Q1 2019" Proof Point. <https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research>
19. "BDO's Fall 2019 Cyber Threat Report: Focus on Healthcare" October, 2019. BDO. <https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber-threat-report-focus-on-health>
20. "IT threat evolution Q1 2019. Statistics" May 23, 2019. Kaspersky. <https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/>





- 21.** "IT threat evolution Q3 2019. Statistics" November 29, 2019. Kaspersky.  
<https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/>
- 22.** "FORMJACKING: How Malicious JavaScript Code is Stealing User Data from Thousands of Websites Each Month" August 2019.  
<https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-formjacking-deep-dive-en.pdf>
- 23.** "Tax Fraud & "Identity Theft On Demand" Continue to Take Shape on the Dark Web" VMWare.  
<https://www.carbonblack.com/resources/threat-research/tax-fraud-identity-theft-dark-web/>

# Related



[READ THE REPORT](#)

## ENISA Threat Landscape Report **The year in review**

A summary on the cybersecurity trends for the period between January 2019 and April 2020.



[READ THE REPORT](#)

## ENISA Threat Landscape Report **List of Top 15 Threats**

ENISAs' list of the top 15 threats of the period between January 2019 and April 2020.

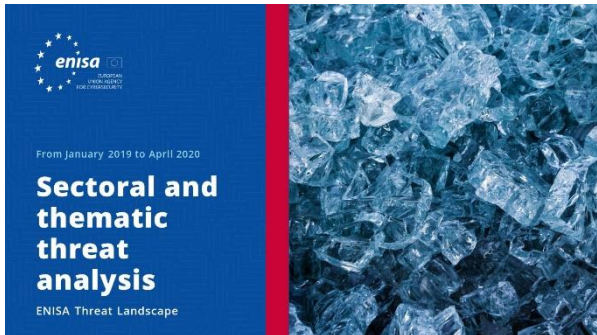


[READ THE REPORT](#)

## ENISA Threat Landscape Report **Research topics**

Recommendations on research topics from various quadrants in cybersecurity and cyberthreat intelligence.





[READ THE REPORT](#)

## ENISA Threat Landscape Report **Sectoral and thematic threat analysis**

Contextualised threat analysis between January 2019 and April 2020.



[READ THE REPORT](#)

## ENISA Threat Landscape Report **Emerging trends**

Main trends in Cybersecurity observed between January 2019 and April 2020.



[READ THE REPORT](#)

## ENISA Threat Landscape Report **Cyber Threat Intelligence overview**

The current state of play of cyberthreat intelligence in the EU.

## – The agency

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at [www.enisa.europa.eu](http://www.enisa.europa.eu).

### **Contributors**

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) and *all members of the ENISA CTI Stakeholders Group*: Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) and Thomas Hemker.

### **Editors**

Marco Barros Lourenço (ENISA) and Louis Marinos (ENISA).

### **Contact**

For queries on this paper, please use [enisa.threat.information@enisa.europa.eu](mailto:enisa.threat.information@enisa.europa.eu).

For media enquiries about this paper, please use [press@enisa.europa.eu](mailto:press@enisa.europa.eu).





## Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

## Copyright Notice

© European Union Agency for Cybersecurity (ENISA), 2020  
Reproduction is authorised provided the source is acknowledged.

Copyright for the image on the cover: © Wedia. For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

**ISBN:** 978-92-9204-354-4

**DOI:** 10.2824/552242



Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Greece  
Tel: +30 28 14 40 9711  
[info@enisa.europa.eu](mailto:info@enisa.europa.eu)  
[www.enisa.europa.eu](http://www.enisa.europa.eu)



All rights reserved. Copyright ENISA 2020.

<https://www.enisa.europa.eu>

