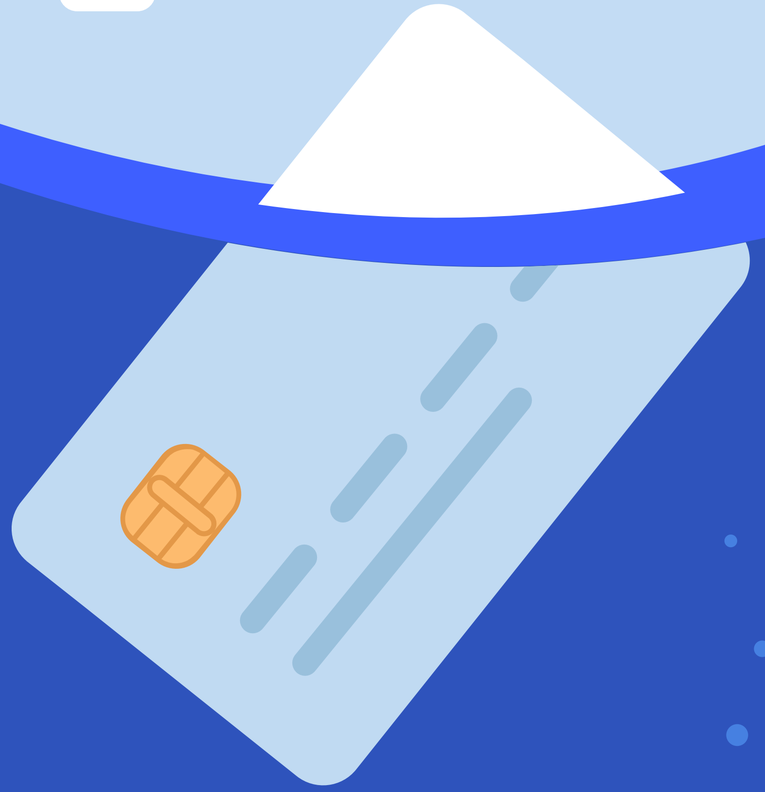
NordVPN®

Tip of the iceberg: 6M stolen cards analyzed



Introduction

Digital systems like payment cards come with inherent security and privacy risks, but our everyday lives are built around the fiction that they are completely trustworthy. What are the real risks of having your card details stolen? What other information is up for grabs by hackers? How can we mitigate those risks?

Card theft is a global problem. The 2020 Nilson Report showed that it led to $28.65 billion in losses around the world, with over one third of the losses centered in the US. Statista found that almost 7% of card sales in the US were fraudulent, predicting that total global losses will reach around $32.96 billion by 2023.

Technology plays a massive role in card fraud and theft. As we showed in NordVPN's research on brute force attacks, computers can be used to guess card details. Payment information may be leaked as a result of data breaches and system hacks. Criminals do not even need to do the dirty work themselves — the dark web hosts thriving marketplaces for stolen card details.

In this report, we present our research into payment card sales on the dark web. Our findings are based on a dataset of almost 6 million cards across eight major markets. We examine the background of how the cards and other personal data were stolen, detailing the methods of our study. We analyze the distribution of stolen cards by country, along with the types of cards available and their prices. We also expand on existing research by examining the connection between stolen card details and other personal information, trying to determine how many card details are hacked, leaked, or stolen instead of using brute-force methods.

Finally, we compare these results with the available population and card penetration data to form a risk index for different countries. We use our findings to provide recommendations for users and businesses on how to prevent the theft of card details and other personal information.

Key takeaways

The dark web marketplaces had the data of 6 million stolen payment cards at the time of our research, with 2.5 million being up for sale for more than $18.5 million in total. If purchased, these payment card details could net criminals much more than they originally paid for them.

US cards are the biggest target — over half of all payment cards discovered came from the US.

Russians were the least likely to find their data on the dark web marketplaces surveyed.

Over 60% of cards were sold alongside other personal information relating to the victim, such as their address, phone number, email address, date of birth, or Social Security number.

Cards sell for an average of $7, but many are leaked for free.

Background

Card fraud often leaves the victim helpless — in large part because it is near impossible to tell how your card details have been stolen. Even security professionals are at risk. But such brute force attacks (guessing the details, confirming them on websites with fewer security checks, then exploiting or selling them on the dark web as detailed in our previous research) are just one way to get payment card details. More direct methods of hacking and theft can make victims feel even more vulnerable — and grab more than just their card details.

Identity theft has been described as "the quintessential crime of the information age." If a data breach or hack exposes not just your card details, but also your address and other personal information, it can lead to more cases of identity theft. Anyone can become a victim of identity theft, and it can take years to undo the damage. Once the attacker has obtained the victim's name, home address, and email address, they may even abuse legal methods (such as using the GDPR's right to access for more personal information) in furthering the identity theft scheme or committing other malicious activities.

Furthermore, while credit card fraud tends to affect wealthier individuals (leading to its portrayal as a "victimless crime" in popular culture because the victims are privileged and credit card companies often refund fraudulent charges), other forms of identity theft like bank account theft often affect the underprivileged.

In this study, we focus on cases where the card details are sold on the dark web alongside other personal information. This ups the stakes, providing additional value (using the information for identity fraud), but it also causes additional harm to the victim (more information exposed and greater risk of identity theft). Such bundles of information come from cybersecurity breaches (hacks, leaks, theft) that could be avoided using appropriate protective measures. But to protect ourselves, we must first understand how card details and other information may be stolen.

Credit card and data theft

We've divided the different methods of theft into a loose categories by the type of attack used:

- **Traditional methods**
  - Physical
  - Social
- **Hacking methods**
  - Devices
  - Systems

We have further divided these categories by scale:

- **Small scale:** Tends to operate on an individual basis.
- **Medium scale:** Less targeted, may be long-term with the potential to scale up.
- **Large scale:** Can be easily automated or affects a huge number of people at once.

Of course, these methods of theft can and often do overlap. One method may even lead to another — for example, a data breach leaking email addresses can lead to a large-scale phishing attempt. Phishing itself covers both social attempts and automated digital methods.

	Traditional		Hacking	
	Physical	**Social**	**Devices**	**Online**
Small scale	Card loss or theft Dumpster diving	Shoulder surfing/copying Family or "friendly" fraud	RFID Public wifi	Hacking online bank account
Medium scale	Card skimmer	Scam phone calls	POS malware	
Large scale		Phishing	Malware on device	Brute force Formjacking Data breach

We will examine each of these methods for stealing card details.

Card loss or theft is perhaps the simplest method used, involving the physical loss of the card itself. Victims tend to be alerted to this method sooner than the others in this list.

Dumpster diving has been described as "no tech hacking." It may involve searching for personal data, bank statements, or old credit cards in domestic trash, or raiding corporate waste disposal facilities for sensitive documents holding larger sets of customer data. It may involve social engineering, such as when it leads to identity theft or when behavioral methods are used to gain unauthorized access to confidential waste.

Shoulder surfing or copying is another form of no tech hacking. It involves looking over someone's shoulder on the train or in a busy café to observe their password, card number, or other information. It also includes sales employees copying card details as they take payments. This method of data theft is very low tech, but it is popular and effective for small-scale criminals.

Family or "friendly" fraud often occurs when those close to us abuse access to our personal information and physical cards, but "friendly" fraud may also be perpetrated by dishonest consumers — for example, by making purchases that are later charged back via the consumer's credit card. This practice ends up costing the seller money, which can be particularly damaging for small online businesses.

Card skimming involves criminals adding an extra device to an ATM to copy the victim's card details. Despite having been around for decades, card skimming devices are easy to miss if you're busy or aren't actively looking for them. Different types of card skimmers have varying levels of concealment, with some being quite sophisticated in altering the ATM.

Scam phone calls are one of the earlier examples of social engineering. In such calls, the scammer pretends to be your bank or other trusted organization to trick you into revealing sensitive information. Governments often publish advice and list ways you can report scam phone calls.

Phishing is a widely known method of attack, mixing more traditional cons with digital techniques (such as spam emails or fake sites) to trick victims into divulging their login details, account information, or card number. Phishing manipulates the cognitive vulnerability triggers that play into our expectations. There are steps you can take if you become a victim, but it is best to act quickly.

RFID involves hacking a payment made with a physical card in close proximity. A contactless payment may be copied and relayed to make payments in other countries. Banks have taken steps to curb RFID attacks.

Public Wi-Fi poses serious security issues, especially when working alongside unknown and possibly malicious devices. The public seems to be aware of at least some of these risks, with users resorting to different behavior patterns for protection. For example, many people tend to avoid online banking when on public Wi-Fi — but they still go on other sites (like social media platforms) that could leak important information and result in identity or credit fraud.

The hacking of online bank accounts tends to affect those in already marginalized groups. The increasing links between banks and emerging fintech firms create additional cybersecurity risks. Institutions may promote protective measures in the form of perceived risk, security-promoting interfaces, institutional trust, and reassurances (like money-back guarantees), although they do not necessarily mitigate against the longer-term potential impact and effects of identity theft.

POS malware involves infecting point of sale (POS) devices in shops with viruses that send card details to hackers. These attacks range from targeting specific shops to large-scale hacks when enough POS devices in a large store are compromised. For example, in 2013 the retail chain Target fell victim to this kind of attack. The threat of malware is especially prominent now that stores are moving towards tablet- and phone-based POS, with criminals continuing to improve their methods to avoid detection.

Malware on devices is a common problem with a large "underground economy" of malware as a service. Malware present on your device can scrape data directly, snoop on other apps (acting like a "ghost in the browser"), or otherwise compromise the security of your personal or company device to send data back to the criminals.

Brute force was explored in detail in an earlier study by NordVPN. A brute force attack involves trying various combinations to guess the card's details. These attacks are made easier by the fact that cards from particular countries, card issuers, and banks follow certain patterns. The guesses can be rapidly checked en masse on sites with lax payment security.

Formjacking is a recently discovered form of web-based attack that uses malicious JavaScript and other techniques to take over online forms and leak the data to hackers. Formjacking is difficult to detect and capable of exploiting a wide range of other vulnerabilities in websites and browsers. It becomes more common in the run-up to the winter holiday period as online shopping increases.

Data breaches are a major reputational risk for companies and a real risk for their customers. The 2015 PwC report to the UK government found that not only had the number of incidents increased compared to the year prior but also that their scale and cost had doubled as well — to the extent that for large businesses they should be considered a "near certainty." While some high-profile breaches do make the news, the situation is often misrepresented and misunderstood. Users often end up mistakenly blaming their own habits rather than the breached organization or hackers, and often underestimate the potential effects to them personally even when they know of the general risks. User-friendly tools are essential when it comes to public awareness and action following a breach. For example, password breach notifications can prevent credential stuffing attacks, limiting the effects of identity theft that results from leaks of personal information.

The table above tries to put each attack type discussed into its appropriate category. This study will focus on the highlighted types because they involve more direct digital hacking techniques and may (to an extent) be mitigated using proper behavior and tools.

It is important to stress that all the attack types above can lead to payment card theft as well as wider cases of identity fraud. When more information is leaked alongside card details, it becomes easier for hackers (and those they sell the data to) to cause more long-term harm to their victims.

Methods

To study the extent of online card theft, we worked with a set of details from millions of cards for sale on the dark web. In particular, we examined the cards that came bundled with other personal information to determine how many were hacked or stolen rather than simply brute forced.

Data collection

The data was compiled in partnership with independent researchers specializing in cybersecurity incident research. They evaluated eight key marketplaces on the dark web to retrieve the details of over 6 million cards, including details of the type of card (credit or debit) and other linked personal information. The data NordVPN received from these third-party researchers did not contain any information that relates to an identified or identifiable individual (such as names, contact information, or other personal information). The study did not determine the exact number or analyze the entirety of payment card details sold on the whole of the dark web — NordVPN only examined the set of statistical data provided by independent researchers.

Data cleaning

Given the nature of dark web marketplaces, not all dark web sellers could be fitted into standard data categories or labels. To create a consistent dataset, we excluded entries with incomplete or incompatible data. These excluded records represent less than 1.5% of the total set — around 3,500 were excluded due to errors in loading the data and a further 80,000 due to unsuitable labeling. This left us with a dataset of 5,953,651 cards.

We arranged the data by country where the card was issued. This initially resulted in over 200 categories, which we narrowed down by focusing on the countries that had more than 1,000 cards in their dataset. This was due to a large number of countries having only a handful of cards that skewed the data when making international comparisons. This left us with 98 countries for comparison, a list generally mirroring the countries' populations. The data from the remaining countries was folded into the category of "no/other country" to keep them present in the set.

Data extraction

From our dataset, we extracted the following information, separated by country:

- **Count**
- **Average price**
- **Card**
  - Type: credit, debit, other
  - Brand: Visa, Mastercard, Amex, other
- **Additional information**
  - Home address
  - SSN
  - DoB
  - Phone number
  - Email address

We then calculated the percentage of the cards that were obtained by way of hacking, theft, or data breaches. This was based on the number containing one or more other pieces of information (home address, SSN, DoB, phone number, or email address). The remainder may have been brute forced because they only contain the card data itself. However, the percentage of hacked cards is a conservative estimate — it is likely that at least some card details categorized as “brute forced” were also a result of theft or breach. Meanwhile, the percentage of brute forced cards represents the maximum possible number of brute force instances (it is highly impractical to brute force other pieces of information in addition to the card details).
We compared the statistical card data between countries with UN population stats and the number of cards in circulation by country or region from Visa, Mastercard, and American Express. Using the information below, we created a risk index to compare the chances of citizens from different countries finding their card data on the dark web:

Number of cards in the dataset (N)
Population (P)
Number of cards in circulation per person (C)
The percentage of cards that were definitely stolen by hacking (H)

The final variable was added to account for the additional risk of certain countries being greater targets for hackers. Brute force attacks can potentially affect all countries, while major breaches and hacks tend to focus on specific businesses, locations, or other entities linked to specific countries. The risk index was calculated using the following formula:

$$RI = \frac{N}{P * C} * H$$

With these data types, we were able to analyze country patterns and differences.

Results

Our study shows that large numbers of card details are being stolen alongside other sensitive personal data, posing a significant risk of identity fraud. The details of millions of cards are being leaked for free on dark web markets. The average price of the 2.5 million cards available for sale was $7.01, with the whole studied dataset of stolen details being worth $18.5 million.

The table at the end of this section shows the top 20 countries by the following key metrics: number of cards, average price, and percentage of cards with additional information (minimum requirement for hacked cards) as well as the highest and lowest risk indexes.

Cards

Out of our dataset containing almost 6 million cards, over half were from the US (3,461,444 cards, or 58.1%). This makes sense, considering the US has a higher rate of card penetration, a sizable population, and a strong economy. Next were India (3.7%), the UK (2.8%), and Mexico (2.6%), followed by Brazil, China, France, and Italy — a mix of countries with high populations and strong economies or political reputations.

Out of the 2.5 million cards that were sold on dark web marketplaces, cards from Denmark commanded the highest average price at $11.54 per card. This was followed by cards from Japan, Portugal, and Ukraine, all over $11 on average.

Interestingly, cards from the US were comparatively cheaper — at $6.86, they fell just below the overall average cost of $7.01. Cards from Argentina and New Zealand were the cheapest, averaging less than $2.50. Considering the amount of damage that can be caused with stolen card data and any bundled personal information, this is a shockingly small amount, suggesting that the use of stolen cards could itself be relatively scalable even by those who have obtained the details second-hand from the dark web.

Additional information

Over half (51.5%) of the cards came with addresses, while a significant number came with phone numbers (39.8%) and email addresses (28.7%). Few cards came with a date of birth (2.5%) or a Social Security number (1.8%) — however, this additional information would expose the victim to a significantly higher risk of identity fraud.

Overall, 62.8% (almost two thirds) of the cards came with some form of additional information, indicating hacking, while up to 37.2% were guessed through brute force attacks (remember, this is an upper bound for brute force attacks and a lower bound for hacks). This means that the majority of stolen card details were obtained by one of the hacking methods discussed earlier.

The numbers vary by country. Of particular note is that records without valid country information followed an inverse trend, with almost all entries only containing card details (92.4%). In general, countries with more cards in the dataset had higher rates of cards with additional information, with the exception of China (which possibly bucked the trend due to a lack of integration with global information systems and the closed-off nature of the Chinese internet, online shopping platforms, and banking platforms).

Almost 90% of cards from India came with additional data, exposing Indian victims to wider issues of identity fraud. Generally, European countries and more economically developed countries had higher rates of additional information, showing a loose correlation between the perceived value of the victim and hacking attempts.

Risk index

Using the calculation outlined above, we created a risk index for 98 countries. Our index takes into account the likelihood of one of your cards being on the dark web as well as the extra risks posed by having it sold with additional information.

The countries with the highest risk index (and therefore the greatest risk) were Malta, Australia, and New Zealand. This is potentially due to their association with the EU or the Anglosphere while having smaller populations compared to their financial and political weight. The US was ranked 5th, while Singapore and Hong Kong were 9th and 10th respectively.

On the other end of the spectrum, Russia had the lowest risk score and China was 3rd from last. This matches with the prevailing hypotheses regarding the location of large-scale hacking operations and the purposeful targeting of Anglo-European countries. Other countries lower on the risk index tended to have smaller economies (with the exception of Germany, which was 15th from last).

The risk index does not necessarily correlate to the number of cards in the dataset, showing the importance of taking into account population size, card penetration, and other factors to assess risk. There is also the case of Germany, which despite a strong economy and a sizable population for a European country, had a very low risk rating. This may be due to political and behavioral factors, such as a greater focus on regulations as well as increased security and privacy measures implemented for individuals and organizations.

Top 20 countries by different categories of data

Country	Cards	%
USA	3461444	58.1
India	218053	3.7
UK	164143	2.8
Mexico	156613	2.6
Brazil	144297	2.4
China	114765	1.9
Canada	97552	1.6
France	97032	1.6
Italy	78676	1.3
Australia	65350	1.1
Spain	60173	1
South Africa	46737	0.8
Türkiye	41803	0.7
Chile	30079	0.5
Germany	26558	0.4
Malaysia	22504	0.4
Argentina	16792	0.3
Peru	13968	0.2
Denmark	12468	0.2
Norway	12055	0.2

Country	Avg price
Denmark	$11.54
Japan	$11.07
Portugal	$11.07
Ukraine	$11.02
Slovenia	$10.83
Vietnam	$10.74
Slovakia	$10.64
Chile	$10.55
Saudi Arabia	$10.55
Thailand	$10.27
Singapore	$10.20
Philippines	$10.00
Mauritania	$9.98
Hungary	$9.71
France	$9.42
Uganda	$9.04
Cameroon	$8.98
Italy	$8.90
Russia	$8.62
Brazil	$8.47

Country	% Hacked
India	89.8
Slovakia	86.3
Saudi Arabia	82.8
Portugal	82
Ukraine	82
Chile	81.4
Hungary	79.2
Japan	78.9
Slovenia	77.2
USA	76.8
Iceland	76.3
France	74.9
Bahrain	74.6
Denmark	74.1
Italy	73.3
Russia	73.2
Iraq	72.9
Greece	72.2
Switzerland	72.1
UK	71.9

Country	Risk index
Malta	1
Australia	0.91
New Zealand	0.84
Slovenia	0.82
USA	0.79
Bahrain	0.79
Bahamas	0.78
UAE	0.78
Singapore	0.77
Hong Kong	0.77
Namibia	0.77
Quatar	0.74
Botswana	0.73
Chile	0.72
Puerto Rico	0.72
Eswatini	0.72
Iceland	0.71
Türkiye	0.71
Oman	0.71
Hungary	0.68

Country	RI (lowest)
Russia	0
Pakistan	0.01
China	0.04
Bangladesh	0.06
Venezuela	0.09
Ukraine	0.16
Indonesia	0.16
Egypt	0.18
Benin	0.18
Zimbabwe	0.2
Paraguay	0.21
Iraq	0.26
Vietnam	0.26
Nigeria	0.27
Germany	0.28
Morocco	0.3
Colombia	0.31
Poland	0.31
Mozambique	0.31
Tunisia	0.32

Recommendations

Banking companies can reduce risks through technological means, but this leaves them to deal with invasive and costly monitoring of customers and potentially fraudulent transactions. Similarly, banks and online shops simply cannot control the wider issues associated with identity theft and data breaches. It is often up to the user to protect themselves against these risks by incorporating online privacy and security tools into their daily life.

We recommend reading our guide on how to protect yourself against identity theft or trying these specific steps and using NordVPN tools against specific threats:

VPN for online banking

- Protect your network traffic, especially on public Wi-Fi, to keep your personal and financial information secure.

Threat Protection

- Scan for malware during downloads to remove potential threats from both personal and business POS devices.
- Block malicious websites that might leak your data or malicious ads that could attempt formjacking.
- Combined with VPNs and other cybersecurity tools, active threat protection can help protect against phishing attempts by hackers to get victims to reveal private information.

Dark web monitor

- Get alerts if your credentials appear on the dark web following a brute force attack or a data breach, giving you a heads up and preventing criminals from getting a head start.

NordPass

- Use unique, complex passwords to protect your online banking and other accounts against brute force attacks and other hacking methods.

NordLayer

- Reduce the risk of breaches for your business and protect your (and your customers') data with multi-layered and scalable network protection — especially if you have remote workers.

Because there are different ways for stealing, hacking, or leaking card details or personal data, it's best to take a multi-pronged approach to security. Combine these tools to reduce the overall risk of your details being sold on the dark web — and the accompanying long-term consequences of credit and identity theft.

References

Benjamin, G. 2023. Mistrust Issues: How technology discourses quantify, extract and legitimise inequalities. Bristol: Bristol University Press.

Caballero, J., Grier, C., Kreibich, C. and Paxson, V. 2011. Measuring Pay-per-Install: The Commoditization of Malware Distribution. USENIX Security 11: 1-16.

Chothia, T., Garcia, F.D., de Ruiter, J., van den Breekel, J., Thompson, M. 2015. Relay Cost Bounding for Contactless EMV Payments. Financial Cryptography and Data Security: 1-18.

Copes, H., Kerley, K.R., Huff, R. and Kane, J. 2010. Differentiating identity theft: An exploratory study of victims using a national victimization survey. Journal of Criminal Justice 38(5): 1045-1052.

Crail, C. 2022. How to Spot a Credit Card Skimmer. Forbes.

Dharmavaram, V.G. 2021. Formjacking attack: Are we safe? Journal of Financial Crime 28(2).

Di Martino, M., Robyns, P., Weyts, W., Quax, P., Lamotte, W. and Andries, K. 2019. Personal Information Leakage by Abusing the GDPR "Right of Access". Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019): 371-385.

Gibbs, S. 2022. Scammers guessed my credit card number – and they could guess yours too. The Guardian.

Jarvis, K. and Milletary, J. 2014. Inside a Targeted Point-of-Sale Data Breach. Dell SecureWorks Counter Threat Unit™ Threat Intelligence 773.

Kahn, C.M. and Roberds, W. 2008. Credit and identity theft. Journal of Monetary Economics 55(2): 251-264.

Kaur, S. and Arora, S. 2020. Role of perceived risk in online banking and its impact on behavioral intention: trust as a moderator. Journal of Asia Business Studies 15(1).

Lake, P. and Behling, S. 2010. E-businesses at risk: a look at the impact and control of e-business fraud. Issues in Information Systems 11(1): 280-285.

Long, J. 2008. No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Syngress.

Maimon, D., Becker, M., Patil, S. and Katz, J. 2017. Self-protective behaviors over public Wifi networks. Learning from Authoritative Security Experiment Results (LASER 17): 69-76.

Mayer, P., Zou, Y., Schaub, F. and Aviv, A. 2021. "Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. 30th USENIX Security Symposium (USENIX Security 21): 393-410.

Najaf, K., Mostafiz, M.I. and Najaf, R. 2021. Fintech firms and banks sustainability: Why cybersecurity risk matters? International Journal of Financial Engineering 8(2).

NCSC. 2021. Phishing Scams.

Nilson. 2020. Nilson Report 2020. Issue 1187.

NordVPN Blog. 2023. What is phishing and how to prevent it. NordVPN.

References

NordVPN Research. 2021. No such thing as a personal device? NordVPN.
-- 2022. Analyzing 4 million payment card details found on the dark web. NordVPN.

Provos, N. 2008. The Ghost in the Browser and Other Frightening Stories About Web Malware. 17th USENIX Security Symposium.

PwC. 2015. 2015 Information Security Breaches Survey. HM Government.

Radu, A.I., Chothia, T., Newton, C.J.P., Boureanu I. and Chen, L. 2022. Practical EMV Relay Protection. IEEE Symposium on Security and Privacy: 1737-1756.

Scaife, N., Peeters, C. and Traynor, P. 2018. Fear the Reaper: Characterization and Fast Detection of Card Skimmers. 27th USENIX Security Symposium (USENIX Security 18): 1-14.

Song, X., Chen, C., Cui, B. and Fu, J. 2020. Malicious JavaScript Detection Based on Bidirectional LSTM Model. Applied Sciences 10(10): 3440.

Statista. 2020. Value of fraudulent payment card transactions worldwide from 2021 to 2027.
-- 2021. Fraud losses per 100 U.S. dollars of total card sales worldwide from 2010 to 2020.

Talukder, M.A.I., Shahriar, H. and Haddad, H. 2019. Point-of-Sale Device Attacks and Mitigation Approaches for Cyber-Physical Systems. In Cybersecurity and Privacy in Cyber Physical Systems. ImprintCRC.

Thomas, K., Pullman, J., Yeo, K., Raghunathan, A., Kelley, P.G., Invernizzi, L., Benko, B., Pietraszek, T., Patel, S., Boneh, D. and Bursztein, E. 2019. Protecting accounts from credential stuffing with password breach alerting. 28th USENIX Security Symposium (USENIX Security 19): 1556-1571.

UN. 2018. World Urbanization Prospects. Department of Economic and Social Affairs, Population Dynamics.

van der Heijden, A. and Allodi, L. 2019. Cognitive Triaging of Phishing Attacks. 28th USENIX Security Symposium (USENIX Security 19): 1309-1326.

Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M. and Anderla, A. 2019. Credit Card Fraud Detection - Machine Learning methods. 18th International Symposium INFOTEH-JAHORINA (INFOTEH 2019): 1-5.

Wieffering, T. 2021. Formjackers: Towards an Internet-scale Survey of Credit Card Skimming on the Web. TU Delft.

Wirth, A. 2019. Reviewing today's cyber threat landscape. Biomedical Instrumentation and Technology: 227-231.

Yu, L., Luo, B., Ma, J., Zhou, Z. and Liu, Q. 2020. You Are What You Broadcast: Identification of Mobile and IoT Devices from (Public) WiFi. 29th USENIX Security Symposium (USENIX Security 20): 55-72.

NordVPN®

2023