Mariusz MATACZ

Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Instytut Nauk o Bezpieczeństwie
mm84186@stud.uph.edu.pl
https://orcid.org/0009-0002-3646-0060

Weronika VODIČKOVÁ
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Instytut Nauk o Bezpieczeństwie
wv83851@stud.uph.edu.pl
https://orcid.org/0009-0007-6606-7151

https://doi.org/10.34739/dsd.2023.01.09

ZJAWISKO PHISHINGU W POLSCE

ABSTRAKT: Phishing to stosunkowo nowe zjawisko, szczególnie w obecnej formie. W świetle danych statystycznych phishing to najpopularniejszy typ cyberataku w Polsce, zatem bez wątpienia jest bardzo istotnym przestępstwem wymagającym sporo uwagi. Cyberprzestępcy stosujący phishing tworzą coraz to nowsze sposoby swoich działań i narażają ofiary na ogromne straty finansowe. Celem artykułu jest omówienie zjawiska phishingu w Polsce jako przestępstwa. Aby dokładnie zobrazować to zagadnienie, konieczne jest zapoznanie się z głównymi pojęciami omawianego tematu oraz ukazanie skali zjawiska. Na początku zostaną nakreślone ramy definicyjne środowiska, w którym funkcjonuje phishing, czyli cyberprzestrzeni, oraz będzie przedstawiona liczebność jej użytkowników. Następnie zostanie scharakteryzowane pojęcie phishingu i poddana analizie skala omawianego zjawiska. Podjęto też temat odpowiedzialności karnej sprawców phishingu oraz profilaktyki tego przestępstwa. Problem badawczy niniejszego opracowania brzmi następująco: Jak kształtuje się przestępstwo phishingu w Polsce?, zaś hipoteza badawcza: Wraz ze wzrostem liczby użytkowników sieci Internet zjawisko phishingu stanowi coraz większe zagrożenie w Polsce i istotne wyzwanie dla polskiego cyberbezpieczeństwa. Na potrzeby pracy wykorzystano metodę analizy literatury przedmiotu oraz metodę syntezy – w tym analizę dostępnych statystyk NASK i CERT Polska.

SŁOWA KLUCZOWE: cyberprzestrzeń, cyberprzestępczość, kryminologia, phishing

THE PHENOMENON OF PHISHING IN POLAND

ABSTRACT: Phishing is a relatively new phenomenon, especially in its current form. According to statistical data, phishing is the most popular type of cyberattack in Poland, making it undoubtedly a significant crime that requires much attention. Cybercriminals who use phishing create increasingly sophisticated methods of their activities, exposing victims to enormous financial losses. The aim of this article is to discuss the phenomenon of phishing in Poland as a crime. To accurately illustrate this issue, it is necessary to describe the main concepts of the discussed topic and to demonstrate the scale of the phenomenon. First, the definitional framework of the environment in which phishing operates, namely, cyberspace, will be outlined, and the number of its users will be presented. Then, the concept of phishing will be characterized and the scale of the discussed phenomenon will be analyzed. The topic of criminal liability of phishing perpetrators and the prevention of this crime will be addressed. The research problem of the article is as follows: How does phishing develop in Poland? The research hypothesis is as follows: With the increase in the number of Internet users, the phenomenon of phishing poses an increasingly significant threat in Poland and is a noteworthy challenge for Polish cybersecurity. The method of literature analysis and synthesis, including the analysis of available statistics from NASK and CERT Polska, was used for the purposes of this article.

KEYWORDS: cyberspace, cybercrime, criminology, phishing

WPROWADZENIE

W ostatnich latach obserwuje się bardzo szybkie tempo rozwoju społeczeństwa informacyjnego oraz nowych technologii. Dokonania technologiczne otworzyły nowe horyzonty i umożliwiły różnorodne formy interakcji międzyludzkich. Postęp technologii informacyjnych oraz związana z nim zależność codziennego życia od Internetu prowadzi jednak do powstania wielu nowych wyzwań i zagrożeń w cyberprzestrzeni. Według Biura Bezpieczeństwa Narodowego najczęściej spotykanymi zagrożeniami w cyberprzestrzeni są: ataki z użyciem szkodliwego oprogramowania (malware, ransomware, wirusy, robaki itp.), kradzieże tożsamości, wyłudzenia oraz modyfikacje czy niszczenie danych, blokowanie dostępu do usług (mail bomb, DoS i DDoS), spam (niechciane lub niepotrzebne wiadomości elektroniczne) oraz ataki socjotechniczne. Z wymienionych niebezpieczeństw jednym z najpowszechniej występujących jest odmiana tego ostatniego zagrożenia – phishing. Jest to rodzaj ataku socjotechnicznego, metoda oszustwa, polegająca na podszywaniu się pod godną zaufania osobę, instytucję lub firmę czy jakikolwiek inny podmiot w celu spowodowania, aby ofiara wykonała określone czynności lub w celu wyłudzenia jej danych wrażliwych, by popełnić właściwy czyn przestępny, najczęściej kradzież środków z konta bankowego. Phishing przybiera różne formy, a każdy kolejny przypadek z biegiem czasu zaskakuje ludzką kreatywnością oraz umiejętnościami manipulacji. Przestępstwo to powoduje, że ofiara ponosi ogromne straty finansowe. Najczęściej w wyniku ataku phishingowego ofiary tracą większość bądź nawet wszystkie oszczędności swojego życia. Phishing jest wyjątkowo dotkliwym przestępstwem dla jednostki wśród innych wymienionych cyberataków.

Głównym celem niniejszego opracowania jest omówienie zjawiska phishingu w Polsce jako przestępstwa, zaś problem badawczy został zawarty w następującym pytaniu: Jak kształtuje się przestępstwo phishingu w Polsce? Z kolei hipoteza badawcza brzmi następująco: Wraz ze wzrostem liczby użytkowników sieci Internet zjawisko phishingu stanowi coraz większe zagrożenie w Polsce i istotne wyzwanie dla polskiego cyberbezpieczeństwa. W celu odpowiedzi na problem badawczy i weryfikacji hipotezy zostaną poddane analizie dane statystyczne pochodzące od NASK i CERT Polska.

CYBERPRZESTRZEŃ – RAMY DEFINICYJNE, CHARAKTERYSTYKA

Kluczowe dla dokładnego przedstawienia zjawiska phishingu jest najpierw zdefiniowanie przestrzeni, w jakiej występuje. Cyberprzestrzeń stanowi kolejne środowisko, obok lądowego, morskiego, powietrznego czy też kosmicznego, w którym można prowadzić różne działania, także przestępcze[1]. Od pozostałych czterech odróżnia je sposób powstania. Cyberprzestrzeń w całości wykreował człowiek, tworząc systemy informacyjne i sieci umożliwiające

[1] M. Stempień, *Bezpieczeństwo informacyjne w cyberprzestrzeni. Analiza działań administracji rządowej Stanów Zjednoczonych Ameryki*, [w:] M. Kubiak, R. Białoskórski (red.), *Informacyjne uwarunkowania współczesnego bezpieczeństwa*, Siedlce-Warszawa 2016, s. 83.

komunikację drogą elektroniczną[2]. Zasadniczym składnikiem cyberprzestrzeni, uwzględnianym w wielu definicjach, jest system teleinformatyczny, który określa wszystko, co wiąże się z komputerami. Cyberprzestrzeń jest przestrzenią komunikacyjną tworzoną przez system powiązań internetowych. Tak jak telekomunikacja, cyberprzestrzeń umożliwia użytkownikom sieci łatwy kontakt, również w czasie rzeczywistym. Stanowi przestrzeń do otwartego komunikowania się za pomocą połączonych komputerów i powiązań informatycznych, które pracują na całym świecie. Tak przedstawiona definicja obejmuje wszystkie systemy komunikacji elektronicznej, w tym także klasyczne sieci telefoniczne. Ujęta w ten sposób istota cyberprzestrzeni jest najbliższa zjawisku phishingu, gdyż występuje ono zarówno w sieciach komputerowych, jak i sieciach telekomunikacji.

Istnieje wiele definicji cyberprzestrzeni sformułowanych przez różne instytucje i organy państwowe, jednakże z reguły wszystkie one są ze sobą tożsame. Przedstawione zostaną najistotniejsze z nich. Cyberprzestrzeń według definicji Unii Europejskiej to „złożone środowisko powstałe wskutek interakcji ludzi, oprogramowania i usług w Internecie za pomocą podłączonych do niego urządzeń technicznych i sieci, które nie istnieje w żadnej formie fizycznej”[3]. Natomiast NATO przyjęło, że cyberprzestrzeń jest tworzona nie tylko przez Internet, oprogramowanie, sprzęt i systemy informacyjne, lecz także przez ludzi wykorzystujących owe sieci i przez społeczne interakcje zachodzące wewnątrz tych sieci[4]. Departament Obrony Stanów Zjednoczonych Ameryki określa cyberprzestrzeń jako „domeny w środowisku informacyjnym, składającym się ze współzależnych sieci infrastruktur informatycznych i danych lokalizacyjnych, w tym z Internetu, sieci telekomunikacyjnych, systemów informatycznych, a także wbudowanych procesorów i sterowników”[5]. Polska Rada Ministrów definiuje cyberprzestrzeń w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 jako „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami”[6]. Biuro Bezpieczeństwa Narodowego dodatkowo wyróżnia cyberprzestrzeń RP. Występuje ona w obrębie terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa Rzeczypospolitej Polskiej, tj. placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji[7].

Cyberprzestrzeń to bez wątpienia wyjątkowe i specyficzne środowisko. Obecnie stało się podstawowym kanałem wymiany informacyjnej. Poza sprzętem, oprogramowaniem i systemami informatycznymi, cyberprzestrzeń wymaga też przede wszystkim ludzkich zachowań

[2] A. Nowak, *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe AON” 2013, nr 3(92), s. 6.
[3] Oficjalna strona internetowa Agencji Unii Europejskiej ds. Cyberbezpieczeństwa, https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-emerging-trends-ebook-en-pl.pdf (20.04.2023).
[4] Oficjalna strona internetowa NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf, (20.04.2023).
[5] Słownik Departamentu Obrony Stanów Zjednoczonych, https://irp.fas.org/doddir/dod/dictionary.pdf (26.04.2023).
[6] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, Monitor Polski, poz. 1037, s. 5.
[7] Biuro Bezpieczeństwa Narodowego, *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, s. 8.

uchwyconych za pośrednictwem sieci cyfrowych. Takie interakcje to bogaty zbiór, który odzwierciedla tak samo pozytywne, jak i negatywne aspekty ludzkiej natury, poczynając od autokreacji i autoekspresji, a na działaniach przestępczych kończąc[8].

CYBERPRZESTRZEŃ – STATYSTYKI

Cyberprzestrzeń w świetle danych statystycznych kształtuje się w następujący sposób:

Tabela 1. Populacja i użytkownicy sieci Internet na świecie

Kontynenty	Populacja	Udział populacji	Użytkownicy Internetu	Udział użytk. Internetu w populacji
Afryka	1,394,588,547	17,6%	601,940,784	43,2%
Azja	4,352,169,960	54,9%	2,916,890,209	67,0%
Europa	837,472,045	10,6%	747,214,734	89,2%
Ameryka Łacińska i Karaiby	664,099,841	8,4%	534,526,057	80,5%
Ameryka Północna	372,555,585	4,7%	347,916,694	93,4%
Bliski Wschód	268,302,801	3,4%	206,760,743	77,1%
Oceania i Australia	43,602,955	0,5%	30,549,185	70,1%
SUMA	**7,932,791,734**	**100,0%**	**5,385,798,406**	**67,9%**

Źródło: opracowanie własne na podstawie statystyk Internet World Stats, https://www.internetworldstats.com/stats.htm (26.04.2023).

Według danych Internet World Stats w roku 2023 liczba osób używających sieci Internet wynosi prawie 5,4 miliarda, przy ogólnej populacji na świecie wynoszącej ponad 7,9 miliarda ludzi. Internet World Stats również podaje, że liczba internautów stanowi prawie 68% światowej populacji[9].

Tabela 2. Populacja i użytkownicy sieci Internet w Polsce w 2023 r.

Populacja	Użytkownicy Internetu	Udział użytk. Internetu w populacji
41,48 mln	36,68 mln	88,4%

Źródło: opracowanie własne na podstawie statystyk Digital 2023, https://datareportal.com/reports/digital-2023-poland (26.04.2023).

[8] M. Górka, *Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa*, [w:] T. Dębowski (red.), *Cyberbezpieczeństwo wyzwaniem XXI wieku*, Wrocław 2018, s. 35.
[9] Strona internetowa Internet World Stats, https://www.internetworldstats.com/stats.htm (21.04.2023).

Bardziej szczegółowe dane prezentuje coroczny raport Digital za rok 2023 przygotowywany przez We Are Social i Meltwater, który sporządzany jest również osobno dla każdego państwa. Według zgromadzonych danych z Polski, populacja wynosi prawie 41,5 miliona ludzi. W Polsce jest niemal 36,7 miliona użytkowników Internetu, co stanowi 88,4% całej populacji Polski[10]. W tym momencie warto zwrócić uwagę na przedstawioną dużą liczbę mieszkańców Polski. Może zostać ona wątpliwie potraktowana, należy mieć jednak na uwadze, że na tak dużą populację Polski mogła mieć wpływ wojna na Ukrainie poprzez napływ uchodźców, którzy przez autorów raportu ewidentnie zostali uwzględnieni. Jak widać z przedstawionej statystyki, znacząca większość mieszkańców Polski ma dostęp do sieci Internet. Większa dostępność Internetu i liczba jego użytkowników powoduje, że również większa jest liczba osób narażanych na cyberataki, w tym phishing.

PHISHING – RAMY DEFINICYJNE, CHARAKTERYSTYKA

Phishing jest jednym z przestępstw i zagrożeń występujących w omówionej cyberprzestrzeni. Ważnym dla precyzyjnego przedstawienia zjawiska phishingu jest krótkie zdefiniowanie grupy przestępstw, do której phishing należy. Cyberprzestępczość, określana też przestępczością komputerową, jest działaniami ściśle związanymi z Internetem. W Konwencji Rady Europy o cyberprzestępczości wyodrębniono cztery kategorie cyberprzestępstw:

- Przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów, w tym: nielegalny dostęp do systemu informatycznego, nielegalne przechwytywanie danych, naruszenie integralności danych, naruszenie integralności systemu, niewłaściwe użycie urządzeń;
- Przestępstwa komputerowe, obejmujące fałszerstwo internetowe i oszustwo komputerowe;
- Przestępstwa ze względu na charakter zawartych informacji, głównie przestępstwa związane z pornografią dziecięcą;
- Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych, wynikających z umów międzynarodowych[11].

Phishing w tym przypadku najbliższy jest zapisowi dotyczącemu przestępstwa komputerowego obejmującego fałszerstwa internetowego i oszustwa komputerowego.

W polskim Kodeksie karnym z zachowań penalizowanych związanych z cyberprzestępczością można wyróżnić:

- Nielegalne podłączanie się do sieci telekomunikacyjnej lub przełamywanie albo omijanie elektronicznych, magnetycznych, informatycznych i innych szczególnych jej zabezpieczeń;
- Nielegalne uzyskanie dostępu do całości bądź części systemu informatycznego;
- Zakładanie lub posługiwanie się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem;

[10] Strona internetowa DataReportal, https://datareportal.com/reports/digital-2023-poland (21.04.2023).
[11] Konwencja Rady Europy o cyberprzestępczości sporządzona w Budapeszcie dnia 23 listopada 2001 r.

- Ujawnianie nielegalnie uzyskanej informacji;
- Niszczenie, uszkadzanie, usuwanie lub zmienianie zapisu istotnej informacji albo w inny sposób uniemożliwianie lub znaczne utrudnianie osobie uprawnionej do zapoznania się z nią;
- Niszczenie, uszkadzanie, usuwanie, zmienianie lub utrudnianie dostępu do danych informatycznych albo w znaczącym stopniu zakłócanie bądź uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych;
- Nieuprawnione zniszczenie, usunięcie, uszkodzenie lub utrudnienie dostępu do danych informatycznych albo nieuprawniona zmiana tych danych, w istotnym stopniu zakłócające pracę systemu informatycznego, systemu teleinformatycznego bądź sieci teleinformatycznej;
- Wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom urządzeń albo programów komputerowych przystosowanych do popełniania przestępstw wymienionych powyżej, jak również haseł komputerowych, kodów dostępu bądź innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej;
- Uporczywe nękanie zwane stalkingiem;
- Kradzież tożsamości;
- Oszustwo komputerowe[12].

Phishing w tej sytuacji prawnej zaliczany jest najczęściej do oszustwa komputerowego, penalizowanego w artykule 287, bądź kradzieży tożsamości – w artykule 190a Kodeksu karnego. Nie istnieje zapis prawny bezpośrednio dotyczący phishingu, ale zachowanie to spełnia przesłanki wyżej wymienionych dwóch czynów zabronionych. Wysokość kary dla sprawcy phishingu wygląda następująco: za oszustwo komputerowe w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, według art. 287 §1 Kodeksu karnego, grozi kara pozbawienia wolności od 3 miesięcy do 5 lat. Jak wcześniej wspominano, charakter phishingu sprawia, że można posłużyć się również art. 190a §2 Kodeksu karnego, w myśl którego każdy, kto podszywa się pod inną osobę, wykorzystując jej wizerunek w celu wyrządzenia szkody majątkowej, podlega karze pozbawienia wolności do 3 lat. Dodatkowo można uznać, że sprawcy dopuszczają się także przestępstwa opisanego w art. 267 Kodeksu karnego, który brzmi „każdy, kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do 2 lat”[13].

Europejska Agencji ds. Cyberbezpieczeństwa przy definiowaniu phishingu zaznacza, że jest to wykorzystanie socjotechniki, nazywanej również inżynierią społeczną. Socjotechnika to „szeroki zakres działań, które mają na celu wykorzystanie ludzkiego błędu lub ludzkich zachowań, aby uzyskać dostęp do informacji lub usług. Socjotechnika stosuje różne formy

[12] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. Nr 88, poz. 553 z późn. zm.).
[13] Ibidem.

manipulacji w celu nakłonienia ofiar do popełnienia błędów bądź przekazania wrażliwych lub tajnych informacji”[14]. Natomiast samo pojęcie phishingu tłumaczy jako „kradzież ważnych informacji, takich jak numery kart kredytowych i hasła, za pośrednictwem wiadomości e-mail, socjotechniki lub oszustwa”[15]. Ponadto Europejska Agencji ds. Cyberbezpieczeństwa trafnie zauważa szeroki charakter phishingu i dzieli go na poszczególne rodzaje. Są to: spear-phishing, whaling, smishing oraz vishing. Przedstawione odmiany phishingu kolejno wyjaśnia:

- „phishing – kradzież ważnych informacji, takich jak numery kart kredytowych i hasła za pośrednictwem wiadomości e-mail, socjotechniki lub oszustwa;
- spear-phishing – bardziej wyrafinowana wersja phishingu, której celem są określone organizacje lub osoby, np. podszywanie się pod ministerstwa i wysyłanie do innych agend rządowych informacji nakazujących otwarcie pliku zawierającego złośliwe oprogramowanie;
- whaling – atak typu spear-phishing skierowany do użytkowników na wysokich stanowiskach (dyrektorów, polityków itp.);
- smishing – termin wywodzący się z połączenia słów „SMS” i „phishing”, który pojawia się, gdy informacje finansowe lub dane osobowe ofiar są zbierane za pomocą wiadomości SMS;
- vishing – połączenie phishingu i głosu – występuje, gdy informacje są przekazywane przez telefon, z którego korzystają złośliwi aktorzy technik socjotechnicznych w celu wydobycia poufnych informacji od użytkowników”[16].

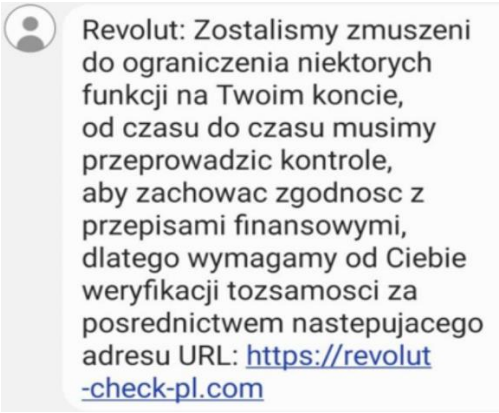
Według Anti-Phishing Working Group najczęściej spotykane motywy związane z phishingiem to działania z użyciem:

- wiadomości e-mail,
- kont Office 365,
- instytucji finansowych,
- aplikacji Microsoft OWA,
- OneDrive,
- kart American Express,
- zestawu ChalBhai,
- konta Adobe,
- Docusign,
- serwisu Netflix,
- konta Dropbox,
- konta LinkedIn,
- konta Apple,
- instytucji pocztowej/firmy kurierskiej,

[14] Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, *ENISA Threat Landscape 2022*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (30.04.2023).
[15] Ibidem.
[16] Ibidem.

– dokumentów Microsoft online (Excel i Word),
– ustawień Windows,
– usługi Google Drive,
– serwisu PayPal[17].

Najpowszechniejszy scenariusz phishingu, który stosują cyberprzestępcy, przedstawia się następująco: na początku atakujący wysyła spam tj. dużą liczbę wiadomości za pomocą poczty elektronicznej, portali społecznościowych, platform handlowych lub SMS do wielu internautów z umieszczonym w treści fałszywym linkiem do spreparowanej strony. Wiadomość ma na celu skłonienie odbiorcy do odwiedzenia konkretnej strony internetowej i podania osobistych danych na przykład loginu wraz z hasłem do swojego konta, na przykład konta bankowego. Spamer często podszywa się pod znaną instytucję, taką jak bank, i przekonuje o konieczności zweryfikowania danych do konta, przy czym link do rzekomej strony internetowej banku niemalże niczym się nie różni od właściwego, oryginalnego adresu internetowego. W zależności od treści wiadomości, ofiara podaje swoje poufne dane bezpośrednio sprawcy albo używa spreparowanej przez cyberprzestępcę strony, przypominającej do złudzenia znaną witrynę i tam podaje swoje poufne dane. W tym momencie zostają one przechwycone przez intruza. Ponadto bywa, że komputer lub smartfon użytkownika zostaje zarażony złośliwym oprogramowaniem, wirusem bądź koniem trojańskim przez pobrany załącznik opisywanej wiadomości. Odtąd intruz jest w stanie kontrolować wszystko, co robi na urządzeniu właściciel sprzętu. Może dokonywać nieuprawnionych transakcji w sposób niezauważalny dla użytkownika, co jest bezpośrednim zagrożeniem dla pieniędzy ofiary[18].



Rysunek 1. Przykładowa wiadomość typu phishing
Źródło: opracowanie własne na podstawie komunikatu Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego polskiego sektora finansowego, https://www.knf.gov.pl/dla_rynku/CSIRT_KNF (24.04.2023).

[17] Anti-Phishing Working Group, *Phishing Activity Trends Report*, 2020, https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf (26.04.2023).
[18] H. Wyrębek, *Cyberprzestrzeń. Zagrożenia. Strategie bezpieczeństwa*, Siedlce 2021, s. 36-37.

PHISHING – STATYSTYKI

Phishing w świetle danych statystycznych kształtuje się w następujący sposób:

Tabela 3. Incydenty obsłużone przez CERT Polska w 2021 r.

Typy incydentu	Liczba incydentów	Udział incydentu w ogólnej liczbie wszystkich incydentów
OSZUSTWA KOMPUTEROWE	**25 472**	**86,40%**
Nieuprawnione wykorzystanie zasobów	3	0,01%
Naruszenie praw autorskich	1	0,00%
Kradzież tożsamości, podszycie się	12	0,04%
Phishing	22,575	76,57%
Niesklasyfikowane	2,881	9,77%

Źródło: opracowanie własne na podstawie statystyk CERT Polska, https://cert.pl/uploads/docs/Raport_CP_2021.pdf (26.04.2023).

Najistotniejszym źródłem danych dotyczących cyberprzestępstw w Polsce jest NASK oraz CERT Polska, która sporządza coroczne raporty ze swojej działalności nazywane „krajobrazem bezpieczeństwa polskiego Internetu". Najnowszy dotąd raport pochodzi z 2021 roku[19]. W 2021 r. CERT Polska zarejestrował 116 071 zgłoszeń. Spośród wszystkich zgłoszeń wytypowanych zostało 65 586, na podstawie których zarejestrowano łącznie 29 483 unikalnych incydentów cyberbezpieczeństwa w Polsce. CERT Polska odnotowuje tendencję wzrostową incydentów bezpieczeństwa. Odnotowano wzrost obsłużonych incydentów na poziomie 182% w porównaniu do roku ubiegłego. Najpopularniejszym typem incydentów w 2021 r. był phishing, który stanowił aż 76,57% wszystkich obsłużonych incydentów. Liczba incydentów zaklasyfikowanych jako phishing w porównaniu do roku poprzedniego wzrosła o 196% i osiągnęła wartość 22 575 incydentów. Zatem wraz ze wzrostem wszystkich incydentów bezpieczeństwa rośnie liczba phishingów, której tendencja wzrostowa jest procentowo większa nawet od ogólnego procentowego przyrostu wszystkich incydentów. Według CERT Polska najpopularniejszym phishingiem w 2021 r. było podszywanie się pod serwis społecznościowy Facebook, co stanowiło 4852 incydentów[20]. Jak widać z przedstawionych danych, phishing został skategoryzowany jako przestępstwo oszustwa komputerowego, które stanowi 86,40% wszystkich incydentów innych kategorii. Oprócz phishingu w tej grupie znajduje się: nieuprawnione wykorzystanie zasobów, naruszenie praw autorskich, kradzież tożsamości, podszycie się

[19] CERT Polska, Raport roczny z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu, 2021, https://cert.pl/uploads/docs/Raport_CP_2021.pdf (26.04.2023).
[20] Ibidem.

i incydenty niesklasyfikowane. Z wymienionej grupy największy udział w tej kategorii incydentu ma phishing, bo aż 76,57%[21].

PHISHING – PROFILAKTYKA

Aby nie zostać ofiarą phishingu, należy przede wszystkim nie panikować i zachować zdrowy rozsądek. Warto zapamiętać kilka podstawowych zasad. Przede wszystkim serwisy internetowe nie wysyłają do swoich klientów wiadomości pocztą elektroniczną ani za pomocą serwisów społecznościowych, Nie powinno się klikać w linki przysłane pocztą elektroniczną ani w załączniki, jeśli nie mamy pewności, kto i w jakim celu przysłał wiadomość. Zwłaszcza jeżeli nie była ona oczekiwana. Stanowi to obecnie najbardziej rozpowszechniony sposób zarażania komputerów wirusami, koniami trojańskimi czy oprogramowaniem szpiegującym. Należy pamiętać, że banki, serwisy aukcyjne i sklepy internetowe używają bezpiecznych połączeń, które wykorzystują certyfikaty cyfrowe oraz szyfrowanie. Warto zatem w trakcie komunikacji np. z bankiem sprawdzić, czy w pasku adresowym przeglądarki pojawia się zielona kłódka. Po kliknięciu na nią powinno otworzyć się okienko potwierdzające, że mamy do czynienia z pożądaną przez nas witryną. Trzeba jednak zaznaczyć, że nie jest to pewnym wyznacznikiem bezpieczeństwa strony, gdyż cyberprzestępcy zaczęli implementować protokół https również do swoich spreparowanych stron[22]. Każdy bank umożliwiający bankowość elektroniczną, ma na swojej stronie porady dla klientów, jak bezpiecznie korzystać z usług online. Oprócz wymienionych zasad, warto na bieżąco aktualizować oprogramowanie oraz wersję przeglądarki, gdyż niektóre metody ataków ulegają stałym zmianom, a producenci oprogramowania starają się za nimi nadążać, publikując nowsze wersje, które bronią się przed znanymi atakami. Na koniec dobrze jest zapamiętać, że danych poufnych nie wolno nigdy podawać w treści wiadomości wysyłanych pocztą elektroniczną czy komunikatorem, ponieważ mogą łatwo wpaść w ręce osób niepowołanych[23].

Zespół CERT Polska działający w strukturach NASK przygotował w 2021 roku elektroniczny dokument z zaleceniami mającymi pomóc użytkownikom Internetu uniknąć padnięcia ofiarą cyberprzestępcy. Zalecenia, które bezpośrednio dotyczą phishingu, to:

- „Logując się na konto zawsze sprawdź, czy domena danego portalu jest prawidłowa. Domena to nazwa zawierająca się między https:// a pierwszym kolejnym znakiem /
- Ignoruj wszystkie inne prośby o podanie swojego hasła, nawet jeżeli komunikat wygląda oficjalnie, wymaga natychmiastowej reakcji i grozi dezaktywacją konta.
- Wszystkie podejrzane wiadomości na skrzynce służbowej zgłaszaj administratorom w swojej organizacji.

[21] Ibidem.
[22] Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, *Wyłudzanie informacji (phishing). Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa*, https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-phishing-ebook-en-pl.pdf (30.04.2023).
[23] H. Wyrębek, op. cit., s. 37-38.

- O wszystkie podejrzane wiadomości na prywatnej skrzynce możesz zapytać CERT Polska (https://incydent.cert.pl / cert@cert.pl).
- Szczególnie podejrzane są wiadomości: zawierające załączniki, a zwłaszcza archiwa i dokumenty Office z hasłem podanym w treści wiadomości; wiadomości zmuszające do podjęcia natychmiastowej reakcji.
- VPN nie chroni przed atakami phishingowymi i złośliwym oprogramowaniem!"[24].

PODSUMOWANIE

Phishing jest przestępstwem od kilkunastu już lat obserwowanym na całym świecie. Od kilku lat proceder ten staje się coraz poważniejszym zagrożeniem przez zwiększoną skalę i swoją szkodliwość. Dotyczy to również Polski. Choć cały czas nagłaśnia się w mediach kolejne przypadki phishingu, liczba ofiar zdaje się nie maleć, a wręcz przeciwnie – wzrastać. Dzieje się tak dlatego, że przestępcy tworzą coraz bardziej kreatywne oraz wiarygodne metody manipulacji, nie zapominając o inteligentnym wykorzystaniu luk prawnych w taki sposób, aby ponieść jak najmniejsze konsekwencje lub nie ponieść ich w ogóle. Prawo polskie nie penalizuje wprost zachowania phishingu, można więc uznać, że nie nadąża za nowymi sposobami wykorzystywanymi przez sprawców cyberprzestępstw. Często przez to większość z nich wciąż pozostaje nieuchwytna, a skradzione pieniądze niemożliwe do odzyskania. W Polsce phishing statystycznie stanowi największe zagrożenie ze wszystkich incydentów zaistniałych w cyberprzestrzeni. Co gorsza, liczba incydentów kwalifikowanych jako phishing z roku na rok wzrasta. Sytuację może w przyszłości zmienić działalność niedawno powstałego Centralnego Biura Zwalczania Cyberprzestępczości Policji oraz podmiotów specjalizujących się w polskim cyberbezpieczeństwie, jak CERT Polska. Na zmianę tę należy jednak jeszcze poczekać. Analiza przedstawionych danych odpowiada jednoznacznie twierdząco na postawioną hipotezę badawczą – wraz ze wzrostem liczby użytkowników sieci Internet zjawisko phishingu stanowi coraz większe zagrożenie w Polsce i istotne wyzwanie dla polskiego cyberbezpieczeństwa.

Największą rolę w przeciwdziałaniu phishingowi odgrywa uświadamianie społeczeństwa, aby ludzie nie ulegali zbyt szybko emocjom i najpierw przenalizowali sytuację, zanim użyją nadesłanego im linku lub podążą za instrukcjami cyberprzestępcy podszywającego się pod na przykład pracownika banku. Ważne jest opisywanie w mediach nowych przypadków oraz tworzenie licznych kampanii społecznych, które uświadomią, jak łatwo zostać ofiarą i jak bardzo trzeba uważać podczas czytania e-maili czy SMSów lub w trakcie rozmów telefonicznych czy używania komunikatorów. Najlepszą ochroną w Internecie są nie tylko programy antywirusowe, ale przede wszystkim zdrowy, ludzki rozsądek.

[24] CERT Polska, *Ważne zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych*, https://cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf (26.04.2023).

BIBLIOGRAFIA

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa. 2022. ENISA Threat Landscape. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa. 2020. Wyłudzanie informacji (phishing). Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa. https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-phishing-ebook-en-pl.pdf.

Anti-Phishing Working Group, Phishing Activity Trends Report. 2020. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf.

Biuro Bezpieczeństwa Narodowego. 2015. Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Warszawa.

CERT Polska. 2021. Raport roczny z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu. https://cert.pl/uploads/docs/Raport_CP_2021.pdf.

CERT Polska. Ważne zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych. https://cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf.

Górka Marek. 2018. Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa. W Dębowski Tomasz (red.), Cyberbezpieczeństwo wyzwaniem XXI wieku. Wrocław: ArchaeGraph, 31-50.

Hoffmann Tomasz. 2018. Wybrane aspekty cyberbezpieczeństwa w Polsce. Poznań: Fundacja na rzecz Czystej Energii.

Hołyst Brunon. 2022. Kryminologia. Warszawa: Wolters Kluwer.

Konwencja Rady Europy o cyberprzestępczości. 2001. Budapeszt.

Nowak Andrzej. 2013. „Cyberprzestrzeń jako nowa jakość zagrożeń". Zeszyty Naukowe AON 3(92): 5-46.

Oficjalna strona internetowa Agencji Unii Europejskiej ds. Cyberbezpieczeństwa, https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-emerging-trends-ebook-en-pl.pdf.

Oficjalna strona internetowa NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.

Olejnik Łukasz, Kurasiński Artur. 2022. Filozofia cyberbezpieczeństwa. Warszawa: Wydawnictwo Naukowe PWN.

Słownik Departamentu Obrony Stanów Zjednoczonych. https://irp.fas.org/doddir/dod/dictionary.pdf.

Stempień Marta. 2016. Bezpieczeństwo informacyjne w cyberprzestrzeni. Analiza działań administracji rządowej Stanów Zjednoczonych Ameryki, W Mariusz Kubiak, Robert Białoskórski (red.) Informacyjne uwarunkowania współczesnego bezpieczeństwa, Siedlce-Warszawa: Wydawnictwo UPH w Siedlcach, 83-98.

Strona internetowa DataReportal. https://datareportal.com/reports/digital-2023-poland.

Strona internetowa Internet World Stats. https://www.internetworldstats.com/stats.htm.

Trejderowski Tomasz. 2013. Kradzież tożsamości. Terroryzm informatyczny. Warszawa: Wydawnictwo ENETEIA.

Trejderowski Tomasz. 2009. Socjotechnika. Podstawy manipulacji w praktyce. Warszawa: Wydawnictwo ENETEIA.

Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, Monitor Polski poz. 1037.
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553 z późn. zm.
Vishwanath Arun. 2022. The Weakest Link: How to Diagnose, Detect, and Defend Users from Phishing. Massachusetts: The MIT Press.
Wyrębek Henryk. 2021. Cyberprzestrzeń. Zagrożenia. Strategie bezpieczeństwa. Siedlce: Wydawnictwo Naukowe UPH w Siedlcach.