DOI: 10.26354/bb.2.1.94.2024

Patryk Król*
ORCID: 0000-0003-4079-8849
patkro12@gmail.com

Phishing jako zagrożenie dla bezpieczeństwa bankowości cyfrowej

Streszczenie

Przedmiot i cel pracy: Celem niniejszego artykułu jest analiza zagrożenia phishingiem, jako głównego wyzwania dla bezpieczeństwa bankowości cyfrowej. Praca skupia się na identyfikacji metod ataków phishingowych, ocenie skuteczności działań obronnych podejmowanych przez instytucje finansowe oraz proponuje rozwiązania mające na celu zminimalizowanie ryzyka dla klientów.

Materiały i metody: Analiza oparta jest na badaniach przeprowadzonych przez różne instytucje, w tym CERT Polska, oraz na analizie konkretnych przypadków ataków phishingowych udokumentowanych przez te organizacje. Zostały wykorzystane również dane statystyczne dotyczące świadomości społeczeństwa w zakresie zagrożeń phishingiem. Metody badawcze obejmują również studium przypadków ataków, analizę przykładów fałszywych stron bankowych oraz propozycje działań prewencyjnych.

Wyniki: Analiza wykazała, że phishing nadal stanowi istotne zagrożenie dla sektora bankowego, a ataki tego rodzaju są często skierowane na klientów instytucji finansowych. Badania pokazują, że mimo działań obronnych podejmowanych przez banki, skuteczność ataków phishingowych utrzymuje się, co wskazuje na potrzebę ciągłego doskonalenia strategii bezpieczeństwa.

Wnioski: Praca sugeruje, że banki powinny kontynuować edukację swoich klientów w zakresie rozpoznawania zagrożeń phishingowych. Ponadto, wprowadzenie dodatkowych metod autoryzacji, jak klucze U2F, może stanowić skuteczną ochronę przed atakami. Warto również zwrócić uwagę na grupy bardziej narażone na ataki phishingowe, takie jak osoby starsze, i dostosować działania edukacyjne do ich potrzeb. Praca wskazuje na konieczność ciągłego dostosowywania strategii bezpieczeństwa banków do ewoluującego krajobrazu cyberbezpieczeństwa.

Słowa kluczowe: pishing, spear pishing, whaling, smishing, vishing, calendar pishing, pharming

Kody JEL: L86

* Patryk Król – Uniwersytet Ekonomiczny w Poznaniu, Katedra Pieniądza i Bankowości.

Phishing as the main threat to digital banking security

Abstract

Subject and purpose of the work: The aim of this article is to analyze the threat of phishing as the main challenge to the security of digital banking. The work focuses on identifying methods of phishing attacks, assessing the effectiveness of defensive actions taken by financial institutions, and proposes solutions to minimize the risk for customers.

Materials and methods: The analysis is based on research conducted by various institutions, including CERT Polska, and on the analysis of specific cases of phishing attacks documented by these organizations. Statistical data on public awareness of phishing threats was also used. Research methods also include case studies of attacks, analysis of examples of fake banking websites and proposals for preventive actions.

Results: The analysis showed that phishing still poses a significant threat to the banking sector, and attacks of this type are often directed at customers of financial institutions. Research shows that despite defensive actions taken by banks, the effectiveness of phishing attacks remains, which indicates the need to constantly improve security strategies.

Conclusions: The work suggests that banks should continue to educate their customers in recognizing phishing threats. Moreover, introducing additional authorization methods, such as U2F keys, can provide effective protection against attacks. It is also worth paying attention to groups that are more vulnerable to phishing attacks, such as the elderly, and adapting educational activities to their needs. The work indicates the need to constantly adapt banks' security strategies to the evolving cybersecurity landscape.

Keywords: pishing, spear pishing, whaling, smishing, vishing, calendar pishing, pharming

JEL Codes: L86

Wstęp

Phishing to popularna metoda oszustwa, polegająca na podszyciu się pod zaufaną osobę lub instytucję w celu wyłudzenia poufnych danych, zainstalowaniu szkodliwego oprogramowania lub nakłonienia phishingowanego podmiotu do wykonania czynności, na której zależy oszustowi (por. Bieńkowska i Falkowski-Gilski 2021). Metoda ta różni się od typowego ataku hakerskiego, w którym cyberprzestępca łamie hasła zabezpieczające dostęp do rachunku bankowego, po czym włamuje się na konto, aby dysponować środkami właściciela, bądź wyrządzić określoną szkodę. Atrakcyjność phishingu dla przestępców wynika z możliwości obejścia zabezpieczeń chroniących rachunki klientów banków, pomimo tego, że w wielu nowoczesnych usługach zabezpieczenia są trudne albo z założenia niemożliwe do złamania

Według Xopero (2021) phishing znalazł się na drugim miejscu wśród zagrożeń w deklaracjach polskich firm (39,8% wskazań po ransomware – 78,2%). Natomiast według KPMG (2024) phishing jest uważany przez większość firm za największe ryzyko cybernetyczne, podobnie jak w ich wcześniejszych badaniach. Z badania SMSAPI (2024) wynika, że phishing jest również dużym zagrożeniem dla klientów;

53,7% respondentów zadeklarowało, iż otrzymało podejrzane treści, a 17,8% iż padło ofiarą oszustwa internetowego. Jak zauważa Ciulkin-Sarnocińska (2015), najczęstszym celem phisherów są banki oraz aukcje internetowe, z kolei najczęstszymi metodami jest rozsyłanie wiadomości e-mail podszywających się pod oficjalne komunikaty banków, zwykle z prośbą o zmianę hasła, odwołanie wysoko wartościowej płatności etc. Często komunikaty te zawierają błędy, z których do najczęstszych należą proste błędy ortograficzne i składniowe. Dzięki temu ofiara może już na początku oszustwa rozpoznać prawdziwego nadawcę wiadomości. Maile phishingowe są zwykle wysyłane z adresów podszywających się pod prawdziwą instytucję[1].

Banki przeciwdziałają phishingowi głównie w sposób defensywny,. poprzez informowanie użytkowników o zagrożeniach, w komunikatach lub na stronach logowania do bankowości elektronicznej (np. PKO BP, Pekao, ING, Santander, VeloBank, Millenium, grupa SGB oraz Bank Spółdzielczy w Brodnicy i Krakowski Bank Spółdzielczy). Działania informacyjne na stronach logowania podejmują również inne instytucje finansowe, jak spółdzielcze kasy oszczędnościowo-kredytowe korzystające z systemu eSKOK. Natomiast w niektórych bankach nie ma takich komunikatów na stronie głównej, gdyż odpowiednie informacje wymagają skorzystania ze specjalnego linku. Te ostatnie rozwiązania są niebezpieczne zwłaszcza dla osób mniej obeznanych z techniką korzystania z bankowości elektronicznej.

Rozwój cyberprzestępczości jest co najmniej paralelny do rozwoju bankowości internetowej. W przypadku cyberataków Krzysztoszek (2017) rozróżnia ataki na infrastrukturę bankową oraz na infrastrukturę klientów. Kluczowe jest zatem, aby w przypadku ataków, których obiektem jest klient banku, miał on odpowiednią wiedzę i narzędzia, aby się przed nimi uchronić. Rabka (2020) pisze, że osoby 65+ stanowią szczególną grupę ryzyka w kontekście zagrożeń z Internetu, co powinno skłaniać instytucje finansowe do należytej troski o ich właściwe informowanie.

Ostatnio ważne działanie z zakresu profilaktyki i zapobiegania cyberprzestępczości podjęło Biuro Informacji Kredytowej dla swych klientów korzystających z usługi „Alerty BIK". W celu lepszej ochrony klientów BIG przed oszustwami i wyłudzeniami 15 kwietnia 2024 r. uruchomiono nową usługę „ostrzeżenia BIK" w formie mailowych powiadomień o różnych niebezpiecznych zjawiskach w cyberprzestrzeni (np. masowych wyciekach danych, metodach kradzieży danych i pieniędzy stosowanych przez oszustów) oraz podejrzanych firmach działających na rynku finansowym. Oprócz informacji o zagrożeniu wysyłane będą również porady, co należy zrobić w danej sytuacji, nawet jeżeli te zdarzenia nie dotyczą bezpośrednio danego klienta, ale warto, aby wiedział i mógł prawidłowo zareagować na nie. Dodatkową korzyścią jest możliwość udostępniania tych informacji znajomym[2].

[1] Przykłady fałszywych witryn, komunikatów oraz wiadomości kierowanych do ofiar zostaną omówione w osobnym rozdziale.

[2] Regulamin Promocji Ostrzeżenia BIK. www.BIK.pl (dostęp 11.04.2024).

1. Metody ataków phishingowych

Podstawowy atak phishingowy polega na zastosowaniu socjotechnik w celu zmanipulowania ofiary, aby ta przekazała przestępcom potrzebne im dane wrażliwe (Matacz i Vodičková 2023). Choć finalnym celem ataku phishingowego jest najczęściej wyłudzenie pieniędzy, może mieć on również na celu pozyskanie informacji wrażliwych, bądź zainstalowanie złośliwego oprogramowania umożliwiającego następne ataki.

Zasadniczo phishing dzieli się według sposobu przeprowadzenia ataku oraz atakowanego podmiotu.

Ze względu na metodę przeprowadzenia ataku phishing można wyróżnić przede wszystkim:

1) Smishing (SMS phishing) – polega na wykorzystaniu spreparowanych wiadomości SMS (Yeboah-Boateng i Amanor 2014) z użyciem techniki *spoofingu*, której efektem jest wyświetlenie fałszywej nazwy (ID) nadawcy, w celu podszycia się pod określoną osobę, bądź instytucję (Piotrowski i Różanowski 2012).
2) Vishing – polega na telefonicznym wyłudzeniu danych wrażliwych (Laszczak 2019), niekiedy także z wykorzystaniem techniki *spoofingu* (Piotrowski i Różanowski 2012).
3) Quishing – polega na umieszczeniu w kodzie QR zainfekowanego adresu URL (Sharevski, Devine, Pieroni i Jachim 2022), przekierowującego ofiarę do spreparowanej strony wiarygodnej dla niego instytucji (np. finansowej), bądź do strony pobierania zawirusowanego pliku.
4) Calendar phishing – polega na nakłonieniu ofiary do dodania zainfekowanego kalendarza w odpowiedniej aplikacji (np. kalendarz Google). Cyberprzestępcy mogą za pośrednictwem własnego kalendarza wysyłać zaproszenia do zainfekowanych stron (Alghenaim, Bakar i Rahim 2022). Sprzyja temu ustawienie automatycznej akceptacji zaproszeń do kalendarzy, które w niektórych aplikacjach są domyślne.
5) Page hijacking – polega na przekierowaniu użytkownika do spreparowanej przez przestępców zainfekowanej strony, lub strony do której cyberprzestępcy wcześniej się włamali (Thakur i Verma 2014).
6) Pharming – polega najczęściej na podmianie pliku *hosts* (Singh 2011) tłumaczącego nazwy domen DNS na IP. Mimo że użytkownik wpisuje poprawną nazwę domeny (np. pkobp.pl) zostaje przekierowany do domeny o innym adresie IP, ale podobnym lub identycznym wyglądzie strony (Kim, Kang i Kim 2015).
7) AIshing – użycie sztucznej inteligencji, technologii uczenia maszynowego lub zaawansowanych modeli językowych zaczyna być coraz bardziej popularne także wśród cyberprzestępców. W nieodległej przyszłości może być to jedna z najpopularniejszych oraz najtrudniejszych do rozpoznania metod ataków phishingowych.

Ze względu na adresata ataku phishingowego można wyodrębnić dwa rodzaje:

1) *Spear phishing* – to spersonalizowany atak phishingowy (Xu, Singh i Rajivan 2023) polegający na starannie spreparowanych wiadomościach (mogących przybierać zarówno formę e-mail, SMS, połączeń telefonicznych, alertów i innych) zawierających informacje dedykowane specyficznie dla danych osób i organizacji będących celem ataku (Schuetz, Lowry i Thatcher 2016).
2) Whaling (CEO fraud) – to atak podobny do ataku *spear phishing*, ukierunkowany na ważnych pracowników (dyrektorów generalnych, dyrektorów finansowych etc.) oraz zamożnych klientów (Kalaharsha i Mehtre 2021). Atak ten można uznać jako szczególny typ ataku *spear phishing*.

Ze względu na pewne typowe cechy w phishingu wyróżnia się zasadniczo cztery fazy działalności przestępcy (Bieńkowska i Falkowski-Gilski 2021 oraz Alkhalil, Hewage, Nawaf i Khan 2021):

1) Faza planowania – cyberprzestępca zbiera informacje o potencjalnych ofiarach, wybiera cel oraz metodę ataku.
2) Faza przygotowania – cyberprzestępca wyszukuje luki oraz słabe punkty w architekturze cyberbezpieczeństwa atakowanego podmiotu, a także wybiera najbardziej dopasowany środek przekazu.
3) Faza ataku – dochodzi do interakcji cyberprzestępcy z ofiarą lub grupą ofiar w celu skłonienia ich do wykonania pożądanej przez cyberprzestępcę czynności. Atak najczęściej zaczyna się od wiadomości, która ma na celu skłonić ofiarę do kliknięcia w link podobny do oryginalnego.
4) Faza wykorzystania informacji – dochodzi do wykorzystania udzielonych przez ofiarę informacji, lub wytworzonych przez nią luk w zabezpieczeniach systemu (tzw. *backdoor*).

2. Przykłady ataków phishingowych

Warto podkreślić, że metody ataków phishingowych pozostają dość podobne, jednak są systematycznie udoskonalane. W tej części artykułu scharakteryzowano przykłady ataków phishingowych przeprowadzone przez oszustów, jakie zostały udokumentowane przez Zespół Reagowania na Incydenty Bezpieczeństwa (ang. akronim CERT) działający w NASK (Naukowa i Akademicka Sieć Komputerowa) stronę www:niebezpiecznik.pl, zajmującą się zarówno popularyzowaniem wiedzy, jak i szkoleniami z zakresu cyberbezpieczeństwa.

Tabela 1. Linki oryginalnych oraz fałszywych stron bankowych

Link oryginalny	Link fałszywy
https:// ipko.pl	https://iko-pl.pw (niebezpiecznik.pl 2023a)
	https://ipko-zablokowany.net (niebezpiecznik.pl 2023b)
	http://www.ipko.co/ (Konieczny 2014)
	http://www.pkobp-online.com/ (Konieczny 2014)
	http://online-pkobp.net/ (Konieczny 2014)
	http://www.myipko.net/ (Konieczny 2014)
	www.weryfikacja-ipko.cu.cc (niebezpiecznik.pl 2013)
BLIK nie ma oficjalnej strony przeznaczonej do płatności, opiera się na systemach płatności online, jak Przelewy24, PayU czy TPay.	https://link.sv/blik (Konieczny 2022)
https://login.ingbank.pl/mojeing/app/	https://login-ingbank.pl-id891uah1zvav18zbga81b.com (niebezpiecznik.pl 2022a)
https://online.mbank.pl/pl/Login	https://s3.amazonaws.com/sledeniepoljak/2/pl.html (niebezpiecznik.pl 2022b) https://rondo.su/mbanku-poland/ (niebezpiecznik.pl 2022b)

Źródło: opracowanie własne, na podstawie serwisu niebezpiecznik.pl

Fałszywy link zwykle nawiązuje lub jest podobny do oryginalnego, jednak znacznie różni się od oryginalnego. Często fałszywy link wykorzystuje protokół HTTPS, który często nadal błędnie jest uważany za gwarancję bezpieczeństwa. Jak zauważa Guga (2007) zadaniem protokołu HTTPS jest ochrona danych przed przechwyceniem przez osoby niepowołane, jednak hasło użytkownika w protokole HTTP wysyłane jest w sposób jawny, co pozwala na odczytanie go przez osoby niebędące adresatami. Cyberprzestępca, jako właściciel domeny i adresat, zgodnie z działaniem protokołu HTTPS może odczytać przesłane mu hasło.

Kolejnym elementem w przestępczym procesie naruszania cyberbezpieczeństwa jest domena do jakiej prowadzą fałszywe linki. Przykładem tego są domeny należące do Palau (.pw), Wysp Kokosowych (.cc), Kolumbii (.co), Salwadoru (.sv), ale również domen międzynarodowych (.com, .net). Oznacza to, że phishing ma międzynarodowy i masowy charakter (Jancelewicz 2022), a przestępcy liczą, że w dużym zbiorze adresatów wiadomości zaledwie niewielki procent zareaguje zgodnie z ich intencją. Według raportu CERT (2023c) najpopularniejszą domeną wykorzystywaną przez cyberprzestępców była domena: .com (6690 przypadków, tj. 41,59% zgłaszanych domen), .pl (3375 przypadków), .online (592 przypadki), .net (509 przy-

padków), .dev (485 przypadków), .info (435 przypadków), .eu (425 przypadków), .org (416 przypadków), .cfd (397 przypadków), .site (342 przypadki). Według CERT korzystanie z domen .com i .pl wynika najprawdopodobniej z ich popularności, a także stereotypowego zaufania użytkowników. Ma to negatywny wpływ na cyberbezpieczeństwo i rzutuje na skuteczność działań przestępców. Z kolei popularność takich domen, jak np. .xyz, wynika z ich niższej ceny i większej dostępności nazw.

Według informacji niebezpiecznik.pl (2014) tylko w jednym ataku przeciw klientom PKO BP przestępcy próbowali wygenerować ok. 100 transakcji, na średnią kwotę 3000 zł, z czego, niestety, kilkanaście przestępczych transferów było udanych. Wykradzione w ten sposób środki zasilały karty *pre-paid* dzięki którym przestępcy mogli wypłacać pieniądze. W początkowych fazach wyłudzenia danych przestępcy posługiwali się własną stroną, tj. oknem logowania, oraz oknem, w którym proszono o podanie dziesięciu kodów z karty kodów jednorazowych (niebezpiecznik.pl 2013). Po udanej akcji uzyskania kodów przekierowywano ofiarę na prawdziwy adres banku, co tłumaczono koniecznością ponownego zalogowania.

Jak zauważa SMSAPI (2024) najłatwiejszymi do zidentyfikowania dla klientów elementami fałszywej wiadomości są:

- ponaglenie do działania zawarte w wiadomości, zwykle z podanym krótkim czasem na reakcję odbiorcy (65,2%),
- nieznany numer, adres lub nazwa nadawcy wiadomości (61,6%),
- zamieszczenie linku (60%),
- brak kontekstu wiadomości,
- niespodziewana wiadomość (58,7%),
- błędy składniowe, ortograficzne, typograficzne (58,6%),
- załączony nietypowy, dziwny adres WWW (58,3%),
- straszenie odbiorcy konsekwencjami (50,2%),
- brak odniesienia do danych odbiorcy (50,2%).

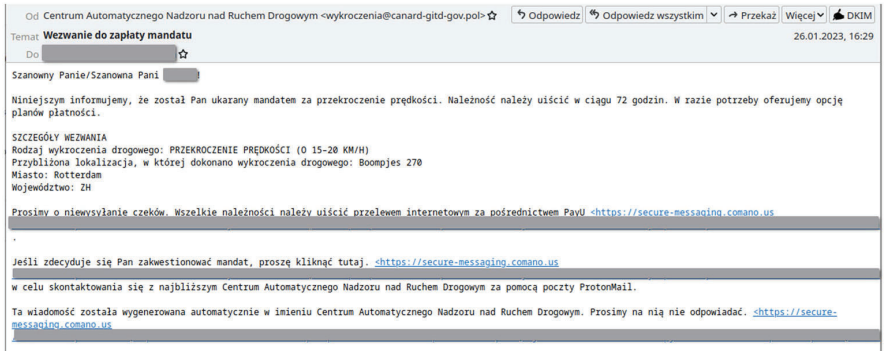
Powyższe cechy wiadomości odnoszą się głównie do podstawowej, masowej formy phishingu. W dobie powstawania coraz bardziej rozbudowanych modeli językowych (np. GPT 4.0, GPT 5.0), z których część dostępna jest bezpłatnie, tworzenie wiarygodnych wiadomości eliminujących te podejrzane staje coraz łatwiejsze. Dlatego profilaktyka, prewencja i zapobieganie oszustwom phishingowym powinny uwzględniać nie tylko te znane, ale także te potencjalne formy phishingu uwzględniające zastosowanie zaawansowanych modeli językowych, nagrań obrazu i głosu wygenerowanych przy użyciu uczenia maszynowego itp. Tym bardziej, że w zasadzie bez ograniczeń dostępne są narzędzia pozwalającego spreparować nagranie z wizerunkiem lub głosem danej osoby. Mają jednak jeszcze stosunkowo łatwo identyfikowane wady (np. charakterystyczna chrypa wygenerowanego głosu, zniekształcenia obrazu przy dynamice postaci, ręki przykładanej do wygenerowanej komputerowo twarzy). Niestety, są już także dostępne bardziej zaawansowane technologicznie narzędzia, dające wyższą jakość generowanego materiału o wyższych kosztach nabycie. Obecnie media publikują już przypadki oszustw z wykorzystaniem sklonowanego głosu (Stefanicki 2023).

Rysunek 1. Post oszustów podszywających się pod Bank Pekao w serwisie Facebook

Źródło: CERT Polska, 2022.

Łatwo zidentyfikować, że w opisach występują czcionki typowe dla cyrylicy, które wkomponowano w treść edytowaną w czcionkach łacińskich. Zabieg ten miał na celu uniknięcie automatycznego wykrycia przez administrację portalu banku. Warto dodać, że domena .icu, która została użyta w tym ataku należy do prywatnej chińskiej firmy Alibaba.

Rysunek 2. Przykład maila phishingowego

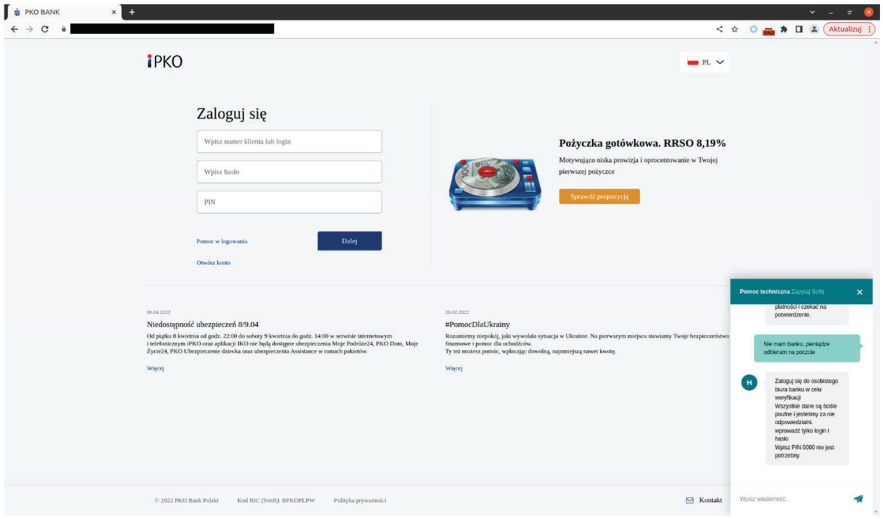


Źródło: CERT Polska, 2023a

Treść maila z rysunku 2 jest przykładem masowego phishingu. Mail jest w wielu miejscach niedopracowany, potencjalna ofiara może zidentyfikować go m.in. po dziwnym adresie e-mail nadawcy, podejrzanych linkach, ponagleniu do wykonania transakcji oraz nieistniejącej instytucji, pod jaką podszywa się nadawca. Ponadto, mail odnosi się do rzekomego wykroczenia drogowego popełnionego w Rotterda-

mie „w województwie ZH", podział administracyjny Królestwa Niderlandów opiera się jednak na prowincjach. Prawdopodobnie wiadomość była szablonem skierowanym do wielu odbiorców w różnych krajach, a odniesienie się w treści do holenderskiego województwa było próbą dostosowania wiadomości do polskiego odbiorcy, zarazem próbą uwierzytelnienia maila w oczach ofiary poprzez zawarcie szczegółowych danych.

Rysunek 3. Przykład fałszywej strony logowania



Źródło: CERT Polska 2023b.

Na fałszywej stronie internetowej banku (rys. 3) widoczny jest przede wszystkim niepasujący graficznie element czatu z „pomocą techniczną". Adresat napisał (dolny prawy prostokąt), że nie ma konta w banku, a pieniądze odbiera na poczcie, a najprawdopodobniej otrzymał automatyczną odpowiedź z poleceniem zalogowania, zapewnieniem o poufności i „odpowiedzialności o dane" banku, oraz informację, że podanie numeru PIN nie jest konieczne. Uważni klienci wiedzieli, że bank PKO BP nie wymagał w pierwszym kroku do logowania w bankowości internetowej numeru PIN, ponadto konieczne do zalogowania hasło pojawiało się dopiero w następnym kroku i na oddzielnej stronie wraz z wybranym przez klienta obrazkiem, stanowiącym jedno z zabezpieczeń przed wyłudzeniem danych.

3. Poziom zagrożenia phishingem w sektorze bankowym w Polsce

Badania Piłata, Pawłowskiego i Kozieła (2022) wskazują, że 77% Polaków nie wie, czym jest phishing. Natomiast największą znajomość phishingu wykazali respondenci w grupie wiekowej 20–24 lata (43%) Autorzy prezentują także reakcje respondentów na prośbę o ocenę, czy przedstawiony im przykład wiadomości mailowej jest wiadomością o charakterze phishingowym. Tylko 27% respondentów odpowiedziało poprawnie, 68% respondentów nie potrafiło udzielić poprawnej odpowiedzi, a 5% zareagowało błędnie. Niski stan świadomości o zagrożeniach atakiem phishingowym potwierdza raport SMSAPI (2024), z badania polegającego na rozpoznaniu oryginalności komunikatu. 30% respondentów wskazało wszystkie trzy fałszywe komunikaty, 47% wskazało wszystkie wiadomości jako fałszywe, 53% wskazało prawdziwą wiadomość jako fałszywą. Jednocześnie aż 62 badanych zadeklarowało, że potrafi rozpoznać fałszywy komunikat. Scharakteryzowane wyniki badań uświadamiają konieczność intensywnej edukacji klientów w zagadnieniach cyberbezpieczeństwa, gdyż w przypadku ataku phishingowego to klient banku stanowi najsłabsze ogniwo łańcucha bezpieczeństwa.

W 2022 r. CERT Polska (2023c) zarejestrował 25 625 incydentów o charakterze phishingu, co stanowiło 64% wśród wszystkich obsłużonych przez CERT incydentów. Przy czym najczęściej wykorzystywana była marka InPost (5119 incydentów), Facebook (4370 incydentów) oraz Vinted (2926 incydentów). Również Zespół CSIRT KNF realizujący zadania Sektorowego Zespołu Cyberbezpieczeństwa, we współpracy z podmiotami krajowego systemu cyberbezpieczeństwa, a w szczególności zespołami CSIRT poziomu krajowego, wspiera Operatorów Usług Kluczowych w obsłudze poważnych incydentów występujących w tych podmiotach, a także prowadzi działania mające na celu analizę pozostałych incydentów, trendów i zagrożeń w obszarze cyberbezpieczeństwa. Instytucja ta (CSIRT KNF 2023) potwierdza, że phishing jest najczęściej stosowaną metodą kradzieży środków finansowych.

3.1. Główne metody zapobiegania phishingowi

Masowość i kreatywność cyberprzestępców wymaga przeciwdziałania ich zamierzeniom czy działaniom na wszystkich fazach phishingu. Utrudnienie planowania phishingu wymaga ograniczenia dostępu do danych wrażliwych, w tym także dotyczących codziennego życia prywatnego klientów. Chodzi o to, aby cyberprzestępca miał jak najmniejszą szansę na uwierzytelnienie siebie dzięki znajomości informacji o potencjalnej ofierze ataku (np. różne próbki głosu służące do wygenerowania potrzebnego komunikatu). Przeciwdziałając intencjom przestępcy w fazie przygotowania ataku, potrzebne jest minimalizowanie luk bezpieczeństwa, zarówno luk oprogramowania, jak i sprzętowych. Służą temu terminowe aktualizacje czy zapory sieciowe (*firewall*). W fazie ataku cyberprzestępca nawiązuje pośredni lub bezpośredni kontakt z ofiarą, co wymaga z jej strony zachowania ostrożności wynikającej m.in. z posiadanej wiedzy

o zagrożeniach. Przede wszystkim minimalizowanie dostępu do informacji o ofierze, a także gotowość i umiejętność zweryfikowania wiedzy przestępcy na swój temat. W ostatniej fazie kluczowa jest rola instytucji finansowych w doskonaleniu identyfikacji prawdziwości danych (w tym kody autoryzacyjne) w trakcie ataku. Przy czym trzeba pamiętać, że w świetle przepisów prawa udostępnienie takich danych komukolwiek kto nie jest właścicielem rachunku bankowego wyłącza odpowiedzialność instytucji finansowych (Popik i Gryglicka 2022).

Niemniej ważne jest również budowanie przez banki, wspólnie z instytucjami sieci bezpieczeństwa finansowego oraz okołobankowymi kultury cyberbezpieczeństwa. Można nawet spotkać opinie, że kultura cyberbezpieczeństwa może w przyszłości stać się nadrzędnym zbiorem wartości wobec wszelkich innych norm dotyczących bezpieczeństwa państwa i obywateli (Górka 2018). Zidentyfikowane trendy zagrożeń cyberbezpieczeństwa wymagają skoordynowanej działalności szkół wszystkich szczebli, a uwzględniając koncepcję uczenia się przez całe życie (ang. *long life learning*) także tzw. edukacji trzeciego wieku. Przykładem działań w tym zakresie podejmowanych przez sektor bankowy jest m.in. projekt „Bezpieczeństwo w Cyberprzestrzeni" realizowany przez Warszawski Instytut Bankowości wraz z partnerami (Visa, Santander, Fundacja Polska Bezgotówkowa, mBank, Allegro oraz Bank Pekao). Warto zwrócić uwagę, że jednym z podmiotów jest firma Allegro, która nie jest częścią sektora finansowego. Może to wynikać z faktu, że wiele ataków phishingowych nakierowanych jest na klientów Allegro. Projekt jest kierowany głównie do studentów (95 tysięcy uczestników) oraz seniorów (8 tysięcy uczestników) (ZBP 2022). Działania na rzecz edukacji w obszarze cyberbezpieczeństwa podejmuje również CSIRT KNF, a są one adresowane głównie do sektora finansowego (CSIRT KNF 2023). Cyberbezpieczeństwo może być też jednym z obszarów międzypokoleniowego uczenia się, jak zauważa Rojek (2019) potencjał uczenia międzypokoleniowego w zakresie cyberprzestrzeni jest duży, lecz nie jest w pełni wykorzystany. Dalej wywodzi on, że międzypokoleniowe uczenie należy animować, wspierać i stwarzać korzystne dla niego warunki wykorzystując narzędzia ICT (technologie informatyczno-komunikacyjne). Oleksiewicz (2019) natomiast eksponuje ważną rolę w kształtowaniu obywatelskiej kultury bezpieczeństwa, m.in. poprzez samokształcenie w zakresie bezpieczeństwa w sieci.

Ponadnarodowy charakter z perspektywy legislacyjnej jest ważnym wydarzeniem dla zwiększania poziomu cyberbezpieczeństwa, dowodzi uchwalenie i wdrożenie dyrektywy PSD2. Przepisy dyrektywy mają na celu wprowadzenie wyższego poziomu bezpieczeństwa podczas przeprowadzania transakcji oraz umożliwienie powstawania innowacji płatniczych; wyrażają również obawy co do możliwego spadku liczby transakcji ze względu na wprowadzone zabezpieczenia (Grzywacz i Jagodzińska-Komar 2018). Jagodzińska-Komar (2016) zauważa również, że na dostawców usług płatniczych został nałożony obowiązek silnego uwierzytelniania klientów (SCA), metoda ta wymaga użycia specjalnych urządzeń cyfrowych (token, karta elektroniczna) lub mechanizmów cyfrowych (klucze kryptograficzne, certyfikaty cyfrowe). Metoda ta łączy się przeważnie z hasłem, dzięki czemu w przypadku kradzieży urządzenia staje się ono bezużyteczne. Silne uwierzytelnianie – w myśl

dyrektywy PSD II – wymaga dwóch, spośród trzech, elementów weryfikujących klienta (np. hasło, kod PIN), posiadanie (np. telefonu komórkowego), cechy klienta (np. cechy biometryczne) (Gradzi 2017). Z obowiązku silnego uwierzytelniania Europejski Urząd Nadzoru Bankowego zwolnił płatności niskokwotowe. Hałasik-Kozajda i Olbryś (2021) zwracają uwagę, że wdrożenie dyrektywy PSD2 w obszarze cyberbepieczeństwa może generować dotkliwe dla mniejszych instytucji finansowych koszty. Kotliński (2022) twierdzi, że jednym z rozwiązań ograniczenia kosztów, tworzenia, rozwoju i bieżącej obsługi systemów IT w bankowości spółdzielczej mogłoby być tworzenie systemów informacyjnych obejmujących cały sektor bankowości spółdzielczej, nie zaś pojedyncze banki, a nawet zrzeszenia.

Jednym z najbezpieczniejszych narzędzi autoryzacji są klucze U2F oraz hasło jednorazowe ograniczone czasowo (OTP). Algorytmy OTP dzielą się głównie na dwa rodzaje, HOTP (HMAC-based One-time Password), czyli algorytm w którym najważniejszą zmienną jest wygenerowane hasło, które pozostaje aktywne do czasu wysłania kolejnej prośby do serwera o wygenerowanie nowego hasła, oraz TOTP (Time-based One-time Password), w którym po określonym, z góry ustalonym czasie staje się nieważne (Digital Fingerprints 2022). Obecnie jedno z narzędzi autoryzacji korzystającym z TOTP, jakim jest token, jest w praktyce dla klientów indywidualnych niedostępny, ze względu na wymóg podania klientowi przed zaakceptowaniem transakcji informacji o jej kwocie i odbiorcy (Samcik 2019). Większość dotychczas stosowanych tokenów (tokeny RSA) była zdolna wyświetlić jedynie kod autoryzacyjny. Część banków (np. Millenium, Credit Agricole) oferuje obecnie tokeny sprzętowe nowego typu, oparte na technologii Cronto (Zagańczyk 2019), która wykorzystuje podobne graficznie do kodów QR graficzne kryptogramy, składające się z matrycy kolorowych kropek, wyświetlanych na ekranie komputera, które następnie można zeskanować tokenem sprzętowym. Bank Credit Agricole oferuje token sprzętowy zarówno dla firm, jak i klientów indywidualnych, zgodnie z tabelą opłat w zależności od typu konta korzystanie z tokena może być bezpłatne, lub obarczone opłatą 7 zł lub 9 zł (Credit Agricole 2024). W przypadku banku Millenium token sprzętowy jest dedykowany dla klientów bankowości przedsiębiorstw, a korzystanie z niego jest obarczone jednorazową opłatą 200 zł za wydanie urządzenia (bankmillenium.pl n.d.). Niska dostępność tokenu może wynikać głównie z ich kosztu, konieczności wymiany baterii, a także skomplikowanie urządzenia i częste gubienie ich przez klientów (niebiezpiecznik.pl 2018). Klucz U2F jest kluczem sprzętowym podobnym do nośnika typu pendrive, najczęściej z wyjściem USB, mikro-USB, lub USB typu C. W standardzie protokołu U2F mogą działać również klucze w technologii Bluetooth oraz NFC (Srinivas, Balfanz, Tiffany i Czeskis 2015). Główną wadą kluczy U2F jest konieczność ich zakupu oraz konieczność posiadania urządzenia w celu autoryzacji logowania do innych urządzeń. Klucze te są powszechnie uważane za jeden z najlepszych narzędzi uwierzytelniania logowania (niebezpiecznik.pl 2021). Chociaż wygodniejszym i łatwiejszym do publicznego użytku rozwiązaniem są aplikacje obsługujące algorytmy TOTP, jak np. Google Authenticator, Microsoft Authenticator czy KeePassXc.

4. Propozycje działań banków

Analizy aktywności cyberprzestępców z wykorzystaniem phishingu wskazują, że nadal bazować będą na masowych atakach. Jednakże elastyczność reakcji świata przestępczego nie wyklucza zmiany taktyki i posługiwanie się zaawansowanymi technikami generowania komunikatów o wyższym stopniu wiarygodności dla ofiar poprzez wykorzystywanie indywidualnie dedykowanych przekazów, skierowanych tylko do celowo wybranych osób. W literaturze taką taktykę ataku określa się jako *spear phishing* (Pitera 2017). Biorąc pod uwagę analizę kosztów i efektów, można założyć, że nadal jeszcze wariant masowych ataków będzie dominował dopóki będzie on bardziej dochodowy.

Urząd Komisji Nadzoru Finansowego (UKNF) zaleca wdrożenie uwierzytelniania wieloskładnikowego tożsamości klienta w elektronicznych kanałach dostępu (Pisarewicz i Podlewski 2023). Propozycja ta, mimo że zmniejsza prawdopodobieństwo udanego ataku hakerskiego, nie eliminuje całkowicie problemu ataków phishingowych, ponieważ w takich sytuacjach to użytkownik ujawnia różnorodne kody autoryzacyjne osobom nieuprawnionym.

Stosunkowo dobrą praktyką w zakresie przeciwdziałania phishingowi jest możliwość weryfikacji danego pracownika lub połączenia telefonicznego na oficjalnej stronie banku lub w aplikacji banku. Takie rozwiązanie obecnie ma w swojej ofercie PKO BP (pkobp.pl 2022) oraz mBank (mbank.pl 2023), polega ono na przekazaniu klientowi danych pracownika w oficjalnej aplikacji danego banku oraz wymogu zatwierdzenia rozmowy telefonicznej z doradcą. W ten sposób potwierdzana jest również tożsamość klienta, dzięki czemu możliwa do uniknięcia jest mało wygodna metoda autoryzacji polegająca na przekazaniu ustnie numeru PESEL, nazwiska panieńskiego matki lub innych danych wymaganych do autoryzacji.

Bardziej zaawansowanym rozwiązaniem w zakresie ochrony przez phishingiem jest stosowanie kluczy U2F. Warto rozważyć odpowiednią akcję promocyjną i udostępnianie ich klientom na przykład w ramach promocji przy założeniu rachunku bankowego lub dla stałych klientów. Aktualnie koszty podstawowej wersji takiego klucza wynoszą od 150 do 200 zł, a bardziej zaawansowane egzemplarze mogą kosztować do 500 zł. Podstawowa wersja klucza U2F może być atrakcyjnym gadżetem reklamowym, zwiększającym zarazem bezpieczeństwo środków klienta. Obok efektu reklamowego takie działanie daje wizerunek banku jako instytucji troszczącej się o klienta i zapewniającej mu bezpieczeństwo. W pierwszym okresie promocji kluczy U2F, zgodnie z koncepcją krzywej doświadczenia w marketingu, pionierzy mają szansę na uzyskanie przewagi konkurencyjnej.

Klucz U2F jest wdrażany w coraz szerszym asortymencie usług z dostępem internetowym. Prym wiodą tu usługi społecznościowe oraz komunikacyjne prowadzone przez gigantów technologicznych, jak Meta czy Alphabet. Sektor bankowy w Polsce również nie lekceważy tego sposobu zabezpieczenia. Pierwszym bankiem w Polsce, który wprowadził możliwość autoryzacji kluczem U2F, był ING Bank Śląski

(Blikowska 2023). Niestety, metoda ta nie zyskała jeszcze szerszego zastosowania, ale uwarunkowania otoczenia i specyfika działalności w sektorze finansowym niezawodnie wymuszą stosunkowo szybko odpowiednie dostosowania, i to nie tylko w segmencie banków.

Dobrą praktyką w zakresie przeciwdziałania phishingowi jest możliwość weryfikacji danego pracownika lub połączenia telefonicznego na oficjalnej stronie banku lub w aplikacji banku. Takie rozwiązanie obecnie ma w swojej ofercie PKO BP (pkobp.pl 2022) oraz mBank (mbank.pl 2023), polega ono na przekazaniu klientowi danych pracownika w oficjalnej aplikacji danego banku oraz wymogu zatwierdzenia rozmowy telefonicznej z doradcą. W ten sposób potwierdzana jest również tożsamość klienta, dzięki czemu możliwa do uniknięcia jest mało wygodna metoda autoryzacji polegająca na przekazaniu ustnie numeru PESEL, nazwiska panieńskiego matki lub innych danych wymaganych do autoryzacji. Wydaje się również, że bank przy podpisywaniu umowy o prowadzenie konta powinien informować klienta o podstawowych zasadach bezpieczeństwa, możliwościach autoryzacji pracownika banku, a także o wyłączeniu odpowiedzialności banku w przypadku rażącego niedbalstwa ze strony klienta. Informacja ta powinna mieć charakter rozmowy z konsultantem, aby mieć pewność, że klient zapoznał się z informacją oraz w pełni ją zrozumiał.

Podsumowanie

Analiza zagrożeń związanych z phishingiem w bankowości elektronicznej pozwala wyciągnąć kilka istotnych wniosków. Przede wszystkim phishing stanowi realne i aktualne zagrożenie, które nie tylko nie traci na znaczeniu, ale wraz z rozwojem techniki i technologii, a także popularności bankowości internetowej, kreuje nowe formy i metody ataku.

Badania dowodzą, że przestępstwa phishingowe występują głównie w sektorze bankowym, bowiem w przypadku skutecznego ataku przynoszą wysokie korzyści finansowe. Przy czym phishing e-mailowy pozostaje nadal jedną z najczęstszych form dostępu do informacji o ofierze poprzez zdobycie jej zaufania poprzedzające uzyskanie potrzebnych danych.

Banki aktywnie przeciwdziałają zagrożeniom związanym z phishingiem. Wprowadzane są środki ochronne, jak komunikaty ostrzegawcze na stronach logowania, informacje o cyberbezpieczeństwie i edukacja klientów. Korzystają w tym ze wsparcia ogniw sieci bezpieczeństwa finansowego (np. UKNF) czy instytucji okołobankowych (np. BIK, UOKiK). Jednakże wobec dynamicznych zmian, a także wykorzystywania nowinek techniki oraz technologii wykorzystywanych przez cyberprzestępców, konieczne jest ciągłe rozwijanie strategii obronnych.

Scharakteryzowane w artykule przykłady ataków phishingowych pokazują, jak złożone i kreatywne były próby wyłudzenia danych. Wprowadzenie kluczy U2F, jako dodatkowego elementu autoryzacji klienta, stanowi krok w kierunku zwiększenia

bezpieczeństwa, jednakże z badań wynika, że świadomość i edukacja klientów w zakresie rozpoznawania zagrożeń nie idzie w parze z rozwojem zagrożeń i wymaga nowych oraz skutecznych inicjatyw, które *per saldo* okażą się tańsze niż konsekwencje przestępstw cybernetycznych. Na uwagę zasługują segmenty klientów szczególnie podatnych na cyberataki, a zwłaszcza osoby o niższych kompetencjach cyfrowych.

Podniesienie poziomu ochrony dotyczy szybkiego i powszechnego wdrożenia technologii uwierzytelniania wieloskładnikowego oraz promocję kluczy U2F. Wprowadzenie tych rozwiązań nie tylko zwiększy bezpieczeństwo, ale może również zwiększyć zaufanie klientów do instytucji finansowej.

Bibliografia

Alghenaim M.F., Bakar N.A.A., Rahim F.A. (2022), *Awareness of Phishing Attacks in the Public Sector: Review Types and Technical Approaches*, [w:] *International Conference on Emerging Technologies and Intelligent Systems* (pp. 616–629). Cham: Springer International Publishing.

Alkhalil Z., Hewage C., Nawaf L., & Khan I. (2021), *Phishing attacks: A recent comprehensive study and a new anatomy*, „Frontiers in Computer Science", 3, 563060.

Bankmillennium.pl (n.d.), *Nowy wymiar uwierzytelnienia*, https://www.bankmillennium.pl/przedsiebiorstwa/bankowosc-elektroniczna/bank-w-internecie/millenet/bezpieczenstwo/token-sprzetowy-z-czytnikiem (dostęp 15.04.2024).

Bieńkowska D., Falkowski-Gilski P. (2021), *Nauka w świecie cyfrowym okiem młodego inżyniera-phishing w mediach elektronicznych*, Pismo PG.

Blikowska J. (2023), *Banki w końcu zaczynają wprowadzać klucze U2F. Hakerom będzie trudniej* – rp.pl. Rzeczpospolita, https://pieniadze.rp.pl/konta-bankowe/art39376181-banki-polskie-klucze-u2f-hakerom-bedzie-trudniej

CERT Polska (2022), *Kampanie phishingowe wykorzystujące wizerunek banków*, https://cert.pl/posts/2022/04/banki-phishing/ (dostęp 25.12.2023).

CERT Polska (2023a), *Kampanie phishingowe na serwisy pocztowe*, https://cert.pl/posts/2023/04/phishing-webmail/ (dostęp 7.04.2024).

CERT Polska (2023b), *Kampania phishingowa wykorzystująca wizerunek Ministerstwa Finansów*, https://cert.pl/posts/2023/01/phishing-govpl/ (dostęp 7.04.2024).

CERT Polska (2023c), *Raport roczny z działalności CERT Polska 2022 – „Krajobraz bezpieczeństwa polskiego internetu"*, https://cert.pl/uploads/docs/Raport_CP_2022.pdf (dostęp 7.04.2024).

Ciulkin-Sarnocińska K. (2015), *Phishing-specyficzna forma pozyskiwania danych newralgicznych*, [w:] *Współczesne oblicza bezpieczeństwa*, red. nauk. E.M. Guzik-Makaruk, E.W. Pływaczewski (pp. 113–121). Temida 2, przy współpracy i wsparciu finansowym Wydziału Prawa Uniwersytetu w Białymstoku.

Credit Agricole (2024), *Tabela opłat i prowizji kont dla osób fizycznych*, https://static.credit-agricole.pl/asset/t/o/i/toip-indywidualni-01022024_28576.pdf (15.04.2024).

CSIRT KNF (2023), *Cyberzagrożenia w sektorze finansowym*, https://cebrf.knf.gov.pl/images/Cyberzagroenia_w_sektorze_finansowym_2022.pdf (dostęp 7.04.2024).

Digital Fingerprints (2022), *OTP, TOTP i HOTP a ochrona haseł. Co oznaczają te skróty i dlaczego warto je znać?*, https://fingerprints.digital/otp-totp-i-hotp-a-ochrona-hasel/ (dostęp 8.04.2024).

Górka M. (2018), *Kultura bezpieczeństwa w kontekście znaczenia informacji jako elementu społeczno-kulturowego*, „Przegląd Politologiczny", (2).

Gradzi D. (2017), *Bezpieczeństwo płatności elektronicznych jako element cyberbezpieczeństwa państwa–przegląd regulacji prawnych*, „Przegląd Bezpieczeństwa Wewnętrznego", 9(16).

Grzywacz J., Jagodzińska-Komar E. (2018), *Rola banków i sektora FinTech w świetle implementacji dyrektywy PSD2*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace", (2).

Guga D. (2007), *Bezpieczeństwo transakcji elektronicznych wykorzystujących infrastrukturę klucza publicznego*, „Acta Universitatis Lodziensis. Folia Oeconomica", 211.

Hałasik-Kozajda M., Olbryś M. (2021), *Skutki implementacji dyrektywy o usługach płatniczych (PSD2)*, „Bank i Kredyt", 52(3).

Iwańczuk-Kaliska A., Marszałek P., Schmidt K., Warchlewska A. (2021), *Ocena zmian na rynku płatności w Polsce*. Raport opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości (Sygn. Wib Pab 10/2021).

Jagodzińska-Komar E. (2016), *Zmiany w systemie SEPA i wpływ Dyrektywy PSD2 na rynek usług płatniczych*, „Zeszyty Naukowe PWSZ w Płocku. Nauki Ekonomiczne", 1(23).

Jancelewicz J. (2022), *Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych*, „Kwartalnik Trzeci Sektor", (59–60 (3–4)).

Kalaharsha P., Mehtre B.M. (2021), Detecting Phishing Sites--An Overview. arXiv preprint arXiv:2103.12739.

Kim, S., Kang, J.Y. i Kim, Y. (2015), *Countermeasures against phishing/pharming via portal site for general users*, „The Journal of Korean Institute of Communications and Information Sciences", 40(6).

Klucz do (cyber)bezpieczeństwa – Baza wiedzy – Portal Gov.pl. (2022) Baza Wiedzy, https://www.gov.pl/web/baza-wiedzy/klucz-do-cyberbezpieczenstwa-

Konieczny P. (2014), *Uwaga klienci PKO i Citi banku! Trwa potężna kampania phishingowa, z kont skradziono już kilkanaście tysięcy złotych*, Niebezpiecznik.pl, https://niebezpiecznik.pl/post/uwaga-klienci-pko-i-citi-banku-trwa-potezna-kampania-phishingowa-z-kont-skradziono-juz-kilkanascie-tysiecy-zlotych/ (dostęp 25.12.2023).

Konieczny P. (2022), *Uwaga! Ktoś podszywa się pod BLIK*, Niebezpiecznik.pl, https://niebezpiecznik.pl/post/uwaga-ktos-podszywa-sie-pod-blik/ (dostęp 25.12.2023).

Kotliński G. (2022), *Dylematy banków spółdzielczych w dobie rewolucji cyfrowej 4.0 ze szczególnym uwzględnieniem wyzwań w sferze marketingu*, [w:] G. Kotliński (red.), *Bankowość komercyjna i spółdzielcza w Polsce – refleksje po trzech dekadach transformacji. Szkice ku pamięci Doktora Ryszarda Mikołajczaka* (s. 215–238). Poznań: Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu. https://doi.org/10.18559/978-83-8211-152-1/12

KPMG (2024), *Barometr cyberbezpieczeństwa. Na fali, czy w labiryncie regulacji?*, https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2024/02/pl-Raport-KPMG-w-Polsce-Barometr-cyberbezpiecze%C5%84stwa-2024.pdf (dostęp 6.04.2024).

Krzysztoszek M. (2017), *Bankowość elektroniczna w teorii i praktyce*, Komisja Nadzoru Finansowego.

Laszczak M. (2019), *Zarządzanie bezpieczeństwem w erze cyfrowej*, „Bezpieczeństwo. Teoria i Praktyka", 37(4).

Matacz M., Vodičková W. (2023), *Zjawisko phishingu w Polsce. De Securitate et Defensione*, „O Bezpieczeństwie i Obronności", 9(1).

mbank.pl (2023), *Potwierdzaj tożsamość w aplikacji mobilnej*, https://www.mbank.pl/indywidualny/aplikacja-i-serwis/pierwsze-kroki/potwierdzenie-tozsamosci/ (dostęp 25.12.2023).

Niebezpiecznik.pl (2013), *Klienci iPKO – uwaga na phishing!*, https://niebezpiecznik.pl/post/klienci-ipko-uwaga-na-phishing/ (dostęp 25.12.2023).

Niebezpiecznik.pl (2014), *Uwaga klienci PKO i Citi banku! Trwa potężna kampania phishingowa, z kont skradziono już kilkanaście tysięcy złotych*, https://niebezpiecznik.pl/post/uwaga-klienci-pko-i-citi-banku-trwa-potezna-kampania-phishingowa-z-kont-skradziono-juz-kilkanascie-tysiecy-zlotych/ (dostęp 6.04.2024).

Niebezpiecznik.pl (2018), *Dlaczego (nie) warto używać aplikacji mobilnej do autoryzacji przelewów?*, https://niebezpiecznik.pl/post/autoryzacja-mobilna-aplikacja-bank-przelewy/ (dostęp 15.04.2024).

Niebezpiecznik.pl (2021), *Klucze U2F – pytania i odpowiedzi. Dlaczego hakerzy ich nienawidzą i dlaczego warto z nich korzystać?*, https://niebezpiecznik.pl/post/klucze-u2f-pytania-i-odpowiedzi/ (dostęp 8.04.2024).

Niebezpiecznik.pl (2022a), *Uwaga klienci ING!*, https://niebezpiecznik.pl/post/uwaga-klienci-ing/ (dostęp 25.12.2023).

Niebezpiecznik.pl (2022b), *Uwaga klienci mBanku!*, https://niebezpiecznik.pl/post/uwaga-klienci-mbanku-2/ (dostęp 25.12.2023).

Niebezpiecznik.pl (2023a), *Uwaga klienci PKO!*, https://niebezpiecznik.pl/post/uwaga-klienci-pko/ (dostęp 25.12.2023).

Niebezpiecznik.pl (2023b), *Uwaga klienci banku PKO!*, https://niebezpiecznik.pl/post/uwaga-klienci-banku-ipko/ (dostęp 25.12.2023).

Oleksiewicz I. (2019), *Bezpieczeństwo informacyjne w cyberprzestrzeni a stany nadzwyczajne Rzeczypospolitej Polskiej*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie", (33), 144–153.

Piłat K., Pawłowski M.T., Kozieł G. (2022), *Analiza wiedzy o aspektach cyberbezpieczeństwa i logowania dwuetapowego w społeczeństwie*, „Journal of Computer Sciences Institute", 23.

Piotrowski Z., Różanowski K., Gajewski P. (2012), *Bezpieczeństwo połączeń w telefonii PSTN*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki", 6(8).

Pisarewicz P., Podlewski J. (2023), *Cyberbezpieczeństwo polskiego sektora ubezpieczeniowego w kontekście krajowych i unijnych regulacji prawnych*, „Bank i Kredyt", 54(5).

Pitera R. (2017), *Współczesne problemy i zagrożenia cyberbezpieczeństwa w sektorze usług bankowości elektronicznej*, „Przegląd Nauk o Obronności", 2(4).

pkobp.pl (2022), *Weryfikacja pracownika banku w IKO*, https://www.pkobp.pl/klient-indywidualny/aplikacja-iko-ipko/bezpieczenstwo/jak-sprawdzic-czy-dzwoni-pracownik-banku (dostęp 25.12.2023).

Popik A., Gryglicka A. (2022), *Ocena poziomu bezpieczeństwa użytkowników rachunków bankowych i analiza zachowań banków w sytuacji wystąpienia incydentu zagrożenia bezpieczeństwa*, „Finanse i Prawo Finansowe".

Rabka M. (2020), *Internet XXI wieku–pułapka zagrożeń dla dzieci, młodzieży i osób starszych w dobie pandemii Covid-19*, „Współczesne Problemy Zarządzania", 8(1(16)).

Rojek, M. (2019), *Cyberprzestrzeń jako miejsce międzypokoleniowego uczenia się. Przykład projektu „ICT Guides"*, „Problemy Opiekuńczo-Wychowawcze", 579(4).

Samcik M. (2019), *Banki w pośpiechu likwidują karty-zdrapki i… tokeny. Co się stało. że token przestał spełniać wymogi bezpieczeństwa?*, https://subiektywnieofinansach.pl/psd2-likwidacja-karty-zdrapki-token-sms-autoryzacyjny/ (dostęp 15.04.2024).

Schuetz S., Lowry P.B., Thatcher J. (2016), *Defending against spear-phishing: Motivating users through fear appeal manipulations*. In 20th Pacific Asia Conference on Information Systems (PACIS 2016), Chiayi, Taiwan, June.

Sharevski F., Devine A., Pieroni E., & Jachim P. (2022), *Gone Quishing: A Field Study of Phishing with Malicious QR Code*s. arXiv preprint arXiv:2204.04086.

Singh J. (2011), *Detection of Phishing e-mail*, IJCST, 2(1).

SMSAPI (2024), *Bezpieczeństwo cyfrowe Polaków. Oszustwa internetowe i zagrożenia komunikacji mobilnej*, https://www.smsapi.pl/static/files/Bezpieczenstwo_cyfrowe_Polakow-Raport_SMSAPI_2024.pdf (dostęp 6.04.2024).

Srinivas S., Balfanz D., Tiffany E., Czeskis A. (2015), *Universal 2nd factor (U2F) overview*, „FIDO Alliance Proposed Standard", 15.

Stefanicki R. (2023), *„Mamo, miałam wypadek!". Uważaj, bo sztuczna inteligencja klonuje głos i wyłudza pieniądze*, wyborcza.biz, https://wyborcza.biz/biznes/7,177150,30152534,mamo-mialam-wypadek-uwazaj-bo-sztuczna-inteligencja-klonuje.html (dostęp 6.04.2024).

Thakur T., Verma R. (2014), *Catching classical and hijack-based phishing attacks*. In International Conference on Information Systems Security (pp. 318–337). Cham: Springer International Publishing.

Xopero. (2021), Cyberbezpieczeństwo Trendy 2021.

Xu T., Singh K., Rajivan P. (2023), *Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks*, „Applied Ergonomics", 108, 103908.

Yeboah-Boateng E.O., Amanor P.M. (2014), *Phishing, SMiShing & Vishing: an assessment of threats against mobile devices*, „Journal of Emerging Trends in Computing and Information Sciences", 5(4).

Zagańczyk M. (2019), *Bank Millennium wprowadza token sprzętowy z czytnikiem i technologią Cronto firmy OneSpan*, https://www.telepolis.pl/fintech/fintech/bank-millennium-wprowadza-token-sprzetowy-z-czytnikiem-i-technologia-cronto-firmy-onespan (dostęp 15.04.2024).

ZBP (2022), Raport: *Cyberbezpieczny portfel*, https://www.zbp.pl/getmedia/bebff99e-f5b7-4644-aec3-4ad3ff5c970a/Cyberbezpieczny_portfel_2022a (dostęp 7.04.2024).