Dydaktyka Informatyki 19(2024)
ISSN 2083-3156; e-ISSN 2543-9847
DOI: 10.15584/di.2024.19.4
http://www.di.ur.edu.pl

Uniwersytet Rzeszowski

Wojciech Marcin CZERSKI

ORCID: 0000-0002-3951-5752. Dr, Uniwersytet Marii Curie-Skłodowskiej, Wydział Pedagogiki i Psychologii UMCS, Instytut Pedagogiki, Katedra Pedagogiki Resocjalizacyjnej, ul. Głęboka 43, 20-612 Lublin; e-mail: wojciech.czerski@mail.umcs.pl

data złożenia tekstu do Redakcji DI: 4.04.2024; data wstępnej oceny artykułu: 10.04.2024

ROLA MEDIÓW W PRZECIWDZIAŁANIU PRZESTĘPCZOŚCI KOMPUTEROWEJ WŚRÓD OSÓB (NIE)KOMPETENTNYCH CYFROWO

THE ROLE OF THE MEDIA IN COUNTERING COMPUTER CRIME AMONG THE DIGITALLY (IN)COMPETENT

Słowa kluczowe: przestępczość komputerowa, oszustwo, media, kompetencje.
Keywords: computer crime, scam, media, competences.

Streszczenie

Świat cyfrowy przestał być atrakcyjny jedynie dla przeciętnego obywatela. Jak wynika z danych policji, przestępcy coraz częściej przenoszą swoją aktywność do cyberprzestrzeni. Spowodowane jest to między innymi poczuciem anonimowości, jaką złudnie daje im Internet. Z tego też względu coraz częściej narażeni jesteśmy na różnego rodzaju oszustwa z wykorzystaniem nowoczesnych technologii, wśród których wymienić można między innymi *phishing*, *spoofing* czy też oszustwo nigeryjskie. Każde z nich nastawione jest na przejęcie naszych środków finansowych. Dlatego tak ważne jest zaangażowanie się mediów w przeciwdziałanie temu procederowi. Celem artykułu jest z jednej strony omówienie wybranych przykładów przestępczości komputerowej, zaprezentowanie jej skali, jak również zaproponowanie sposobu zaangażowania się mass mediów w ograniczenie tego procederu, zwłaszcza wśród osób starszych.

Abstract

The digital world is no longer attractive only to the average citizen. According to police data, criminals are increasingly moving their activities into cyberspace. This is due, among other things, to the sense of anonymity that the Internet illusorily gives them. For this reason, we are increasingly exposed to various types of fraud using modern technologies, including phishing, spoofing and the Nigerian scam. Each of these is ultimately aimed at intercepting our funds. This is why it is so

important for the media to get involved in fighting and countering this practice. The aim of this article is, on the one hand, to discuss selected examples of computer crime, to present its scale and also to suggest ways in which the media can become involved in curbing it, especially among older people.

Wstęp

Nie ulega wątpliwości, że zarówno Internet, jak i smartfony bardzo ułatwiają codzienne funkcjonowanie każdego człowieka. Coraz więcej firm i instytucji przenosi swoje usługi bądź też rozbudowuje już istniejące w świecie cyfrowym, co ma na celu szybszy i łatwiejszy kontakt z klientem, jak również w pewnym sensie podniesienie jakości życia użytkowników. Przykładami takich usług są aplikacje *mObywatel*[1] oraz *Profil zaufany*[2]. Co jakiś czas przeczytać można lub zobaczyć na tych stronach nowe funkcje czy też możliwości załatwienia spraw urzędowych.

Taka konsolidacja usług cyfrowych w jednym miejscu (nie tylko w samej sieci, ale i urządzeniu) niesie za sobą wiele zagrożeń, na które najbardziej narażone są osoby nieposiadające odpowiednich kompetencji cyfrowych. Jednym z najpoważniejszych zagrożeń dla nich wydają się być oszustwa, które w ostatnich latach są prawdziwą plagą.

Celem artykułu jest przybliżenie, czym jest przestępczość komputerowa, ze szczególnym uwzględnieniem oszustw wykorzystujących nowoczesne technologie, jej skala oraz propozycje działań profilaktycznych, w które głównie powinny zaangażować się media.

Przestępczość komputerowa – problem definicyjny

Jak wskazują niektórzy autorzy, pierwsze wykorzystanie komputerów do celów przestępczych miało miejsce już w latach 60. XX w.[3] Jednak dopiero pod koniec lat 70. opracowana została jedna z pierwszych definicji przestępczości komputerowej, zgodnie z którą są to „wszelkie nielegalne działania, dla których znajomość technologii komputerowych jest niezbędna do pomyślnego oskarżenia”[4]. W 1983 r.

[1] *mObywatel 2.0 – Aplikacja mobilna i serwis dla obywateli*, https://info.mobywatel.gov.pl/ [10.03.2024].

[2] *Profil zaufany – Portal Gov.pl*, https://www.gov.pl/web/profilzaufany [dostęp: 10.03.2024].

[3] I.A. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, „Kortowski Przegląd Prawniczy”, Olsztyn 2017, s. 13; M. Siwicki, *Cyberprzestępczość*, C.H. Beck, Warszawa 2013, s. 9.

[4] J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015, s. 35.

S. Schjølberg analizowane tu pojęcie zdefiniował jako „wszelkie nielegalne działania, dla których znajomość technologii komputerowych jest niezbędna do ich popełnienia”[5]. Jak można zauważyć, w powyższych definicjach nacisk przeniesiony został z organów ścigania na sprawcę dokonanych czynów przestępczych.

Dalszy rozwój prac nad zjawiskiem przestępczości komputerowej doprowadził do opracowania przez ekspertów OECD definicji uznającej ją za „każde zachowanie niezgodne z prawem, nieetyczne lub nieuprawnione, odnoszące się do automatycznego przetwarzania oraz przekazywania danych”[6].

M. Siwicki, analizując pierwsze definicje zjawiska przestępczości komputerowej, zwraca uwagę, że pierwotnie rozumiane było ono dwojako. Z jednej strony obejmuje ono użycie komputera jako przedmiotu bądź też środowiska zamachu. Z drugiej, pojęciem tym określa się wszelkie przestępstwa, „które były popełniane przez osoby o wysokich umiejętnościach i wiedzy z zakresu elektroniki lub informatyki. W tym drugim ujęciu posiadanie przez sprawcę szczególnej wiedzy i umiejętności było traktowane jako istotny element przestępczości komputerowej”[7].

Jak słusznie zauważa K. Witek, „próba stworzenia kompleksowej definicji przestępstw popełnianych z użyciem komputera okazała się wyjątkowo skomplikowana”[8]. Spowodowane jest to między innymi tym, że komputer pełni tu dwojaką funkcję – narzędzia oraz celu[9].

Innym powodem problemów definicyjnych może być fakt, że „przestępstwa komputerowe materializują idee, które w odniesieniu do czynów przestępczych były niegdyś realizowane za pomocą rąk lub narzędzi istniejących w świecie rzeczywistym. Cyberprzestrzeń stała się nową ścieżką, którą podążać zaczęli oszuści w celu szybszego uzyskania jednostronnych korzyści”[10].

Jeszcze innym powodem jest dynamiczny rozwój nowoczesnych technologii, zwłaszcza mobilnych, co również ma ogromny wpływ na zjawisko przestępczości. Z tego też względu część badaczy uważa, że pojęcie przestępczości

---

[5] S. Schjølberg, *Computers and penal legislation: a study of the legal politics of a new technology*, Universitetsforlaget, Oslo 1983.

[6] J. Wasilewski, *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego” 2016, t. 8, nr 15, s. 152.

[7] M. Siwicki, *Cyberprzestępczość...*, s. 10.

[8] K. Witek, *Przestępczość komputerowa – aspekty prawne*, „Edukacja – Technika – Informatyka” 2018, t. 24, nr 2, s. 40.

[9] por. K.J. Jakubski, *Przestępczość komputerowa – zarys problematyki*, „Prokuratura i Prawo” 1996, nr 12, s. 34.

[10] A. Warchoł, *Przestępstwa komputerowe i problemy wojny w cyberprzestrzeni* [w:] *Elementy bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Analiza wybranych systemów*, red. P. Swoboda, A. Żebrowski, Avalon, Kraków 2020, s. 67.

komputerowej „stało się w dzisiejszych czasach zbyt ogólne”[11]. Stąd też coraz częściej w literaturze znaleźć można pojęcie „cyberprzestępczość”, którego celem jest określenie przestępstw popełnianych zarówno za pomocą komputerów, jak również innych urządzeń cyfrowych, a samo pojęcie „przestępczości komputerowej” uznać można za niewystarczające do określenia aktualnych form przestępstw realizowanych w świecie cyfrowym. Zatem dla celów dalszej analizy przyjąć należy, iż *przestępczość komputerowa* to wszelkie zachowania o charakterze przestępczym, do realizacji których wykorzystane są nowoczesne technologie.

Wybrane rodzaje przestępstw komputerowych

Niezależnie od tego, czy przestępstwa ze świata cyfrowego nazywać będziemy ostatecznie *przestępstwami komputerowymi*, czy też jak część autorów za bardziej adekwatne uznamy *cyberprzestępczość*, katalog tego rodzaju czynów zabronionych jest szeroki i obejmuje między innymi: piractwo komputerowe, hakerstwo, cyberterroryzm, wirusy komputerowe, pornografię dziecięcą, handel cyberseksem. Szczególną kategorię stanowią tu przestępstwa skierowane przeciw mieniu, do których zaliczyć można przede wszystkim: kradzież tożsamości, oszustwa internetowe/bankowe, cyberwyłudzenia, oszustwa reklamowe[12]. Natomiast szczególnie dzieci i młodzież narażone są na cyberstalking, cyberprzemoc, wirtualne znajomości, *grooming*, *seksting*[13].

Poniżej omówione i scharakteryzowane zostały coraz powszechniejsze przestępstwa skierowane przeciwko mieniu. Należą do nich między innymi oszustwo (art. 286 k.k.) oraz oszustwo komputerowe (art. 287 k.k.)[14].

Zgodnie z zapisami art. 286 §1 Kodeksu karnego osobie, która „w celu osiągnięcia korzyści majątkowej doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania” grozi od 6 miesięcy do 8 lat pozbawienia wolności.

Natomiast w art. 287 § 1 dotyczącym oszustw komputerowych mowa jest o tym, iż „kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej

[11] K. Witek, *Przestępczość komputerowa – aspekty prawne*…, s. 40.

[12] por. *Cybercrime* [w:] *Wikipedia*, 2022; M.A. Dennis, *Cybercrime – Spam, steganography, and e-mail hacking | Britannica*, https://www.britannica.com/topic/cybercrime [dostęp: 16.01.2022].

[13] por. K. Garwol, *Polska szkoła w dobie zagrożenia cyberprzestępczością*, „Dydaktyka Informatyki” 2018, t. 13; S. Kozak, *Patologie komunikowania w Internecie: zagrożenia i skutki dla dzieci i młodzieży*, Difin, Warszawa 2011.

[14] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 2021, poz. 2345, 2447).

osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5".

Ogólnie oszustwa popełniane przy użyciu nowoczesnych technologii podzielić można na pięć grup:

1. nielegalne transakcje online – np. oferowanie nieistniejących towarów lub wyłudzanie świadczeń na podstawie skradzionych kart płatniczych;
2. zaawansowane oszustwa z opłatami – np. oferowanie opłat za dostęp do nieistniejących stron;
3. przestępstwa związane z elektronicznym transferem środków – np. użycie podstępu celem uzyskania dostępu do konta;
4. oszustwa inwestycyjne – np. fałszywe strony oferujące możliwość szybkiego zysku z inwestycji;
5. kradzież tożsamości[15].

Konkretnymi przykładami działań przestępczych zatem są coraz popularniejsze *phishing*, *spoofing* czy też oszustwo nigeryjskie.

Phishing pochodzi od angielskiego *password harvesting fishing* i dosłownie oznacza łowienie haseł. Jest to metoda polegająca na podszywaniu się najczęściej pod instytucje, np. banki, w celu „zweryfikowania" szczegółowych danych dotyczących naszych danych[16]. Najczęściej przestępcy „wykorzystują wiadomości email rozsyłane w dużej liczbie (analogicznie jak spam), próbując nakłonić potencjalne ofiary do odwiedzenia odpowiednio spreparowanej strony internetowej, która ma przypominać stronę danego banku"[17]. Przygotowana przez przestępców strona, jak i sam email, do złudzenia przypominają prawdziwe. Różnice można jednak dostrzec, dokładnie przyglądając się adresowi strony. Aby zmylić użytkownika przestępcy rejestrują domenę łudząco podobną do tej, pod którą zarejestrowana jest strona banku. W tym celu np. zmieniają jedną literę w jej adresie. Jako „przykład niech posłuży strona banku ING »www.ingbank.pl« i ich poczta »noreply@ingbank.pl«. Fałszywy sposób kodowania to »WWW.lNGBANK.PL« i poczta »NOREPLY@lNGBANK.PL«. Różnica między tymi adresami na pierwszy rzut oka jest niewidoczna, jednak po głębszej analizie okazuje się, że w fałszywym sposobie zapisu adresu zamiast dużej litery »I« występuje mała litera »L«"[18].

---

[15] *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, Wolters Kluwer Polska, Warszawa 2018, s. 459–460.

[16] J. Kosiński, *Paradygmaty cyberprzestępczości*…, s. 126.

[17] R. Maciejczyk, *Bankowość elektroniczna – zagrożenia*, „Kwartalnik Policyjny" 2017, nr 4(43), s. 38.

[18] A. Rogowski, *Phishing*, „Kwartalnik Policyjny" 2017, nr 4(43), s. 57.

Spoofing jest metodą wykorzystywaną w ***Vishingu*** i polega na podszywaniu się przestępcy pod numer telefonu, np. infolinii banku. Podczas rozmowy próbuje on przekonać ofiarę, iż z jej konta próbowano dokonać przelewu, a przestępca udający przedstawiciela banku odkrył to i zablokował. Następnie informuje ofiarę o przełączeniu rozmowy do działu technicznego, gdzie rzekomy pracownik nakłania ofiarę do zainstalowania oprogramowania do zarządzania pulpitem zdalnym oraz jego skonfigurowanie. Jak już ofiara to zrobi, wówczas prosi o zalogowanie się na stronie banku w celu weryfikacji operacji dokonanych na rachunku bankowym, dzięki czemu przestępcy otrzymują dostęp do konta ofiary. Często zdarza się również, że ofiara proszona jest o przekazywanie przestępcy przychodzących kodów weryfikacyjnych[19].

Ostatnim przykładem popularnych oszustw jest tzw. oszustwo nigeryjskie. W literaturze można znaleźć też inne jego nazwy: „spam nigeryjski", „nigeryjski mailing", „oszustwo 419"[20]. Jest to bardzo prosty proceder, wręcz naiwny. Ofiara otrzymuje maila, np. z informacją o transferze ogromnej kwoty pieniędzy, i wciągnięta zostaje w swoistą grę psychologiczną. Typowa fabuła takiego oszustwa oparta jest „na fikcyjnym transferze dużej kwoty pieniędzy (często przesadnie wygórowanej – nawet rzędu kilkunastu milionów funtów lub dolarów amerykańskich) z jednego z krajów afrykańskich […] – mająca na celu wyłudzenie pieniędzy od ofiary zaślepionej wizją zbliżającej się fortuny"[21]. Ofiara najczęściej proszona jest o przekazanie danych osobowych albo środków pieniężnych na pokrycie „kosztów manipulacyjnych" związanych z transferem tych środków[22]. Wśród odmian tego oszustwa spotkać można: „uchodźca polityczny z Czarnego Lądu", „spadek", „konto w banku bez właściciela", „wygrana w loterii" lub „udział w konferencji naukowej"[23].

Skala przestępczości komputerowej w Polsce w latach 2013–2022

Zarówno rozwój Internetu i technologii mobilnych, jak również upowszechnienie się ich praktycznie w każdej grupie wiekowej (zwłaszcza wśród osób starszych) jest jednym z podstawowych elementów determinujących przestępców do przeniesienia swojej aktywności do świata cyfrowego. Poniżej zaprezen-

[19] por. *Vishing*, https://www.knf.gov.pl/dla_konsumenta/kampanie_informacyjne/cyberoszustwa_inwestycyjne/schematy_oszustw/vishing?articleId=87578&p_id=18 [29 marzec 2024 r.].

[20] J. Kosiński, *Paradygmaty cyberprzestępczości...*, s. 112.

[21] M. Siwiecki, *Oszustwa nigeryjskie – próba klasyfikacji*, „Kwartalnik Policyjny" 2017, nr 4(43), s. 50.

[22] J. Kosiński, *Paradygmaty cyberprzestępczości...*, s. 112.

[23] M. Siwiecki, *Oszustwa nigeryjskie – próba klasyfikacji*…, s. 51–54.

towane zostały dane otrzymane z Komendy Głównej Policji dotyczące art. 286 i art. 287 k.k.

Tabela 1. Liczba wszczętych postępowań w związku z wybranymi artykułami k.k.

Rok	Art. 286 § 1–3		%	Art. 287 § 1–2		%
	Wszystkie	Internetowe		Wszystkie	e-bankowość, *phishing*	
2013	73351	14732	20,1	1768	–	–
2014	78681	19862	25,2	2597	767	29,5
2015	83028	24781	29,8	4105	1321	32,2
2016	80475	27296	33,9	4103	1784	43,5
2017	82754	29161	35,2	4554	2340	51,4
2018	81241	30437	37,5	7402	4555	61,5
2019	84009	32627	38,8	10793	7147	66,2
2020	83822	35566	42,4	11219	7834	69,8
2021	102337	49604	48,5	21244	16734	78,8
2022	101719	46200	45,4	26824	21788	81,2

Źródło: opracowanie własne na podstawie danych przekazanych z KGP drogą mailową

Jak widać z danych zaprezentowanych w tabeli 1, w przypadku oszustw penalizowanych w k.k. w art. 286 okres pandemii COVID-19 był kluczowy dla wzrostu przestępczości związanej z wykorzystaniem nowoczesnych technologii. Zarówno w 2021, jak i 2022 r. liczba wszczętych przez policję postępowań dotyczących oszustw dokonanych za pośrednictwem Internetu stanowi niespełna połowę wszystkich postępowań z tego artykułu.

Zwiększenie nacisku na ściganie oszustw komputerowych (art. 287 k.k.) dotyczących bankowości internetowej oraz *phishingu* zaobserwować można już od 2018 r., kiedy to zaczęły one stanowić znacznie ponad połowę wszystkich wszczynanych postępowań.

Tabela 2. Liczba stwierdzonych przestępstw w związku z wybranymi artykułami k.k.

Rok	Art. 286 § 1–3		%	Art. 287 § 1–2		%
	Wszystkie	Internetowe		Wszystkie	e-bankowość, *phishing*	
2013	94048	13607	14,5	1675	–	–
2014	102832	19904	19,4	2312	585	25,3
2015	115123	28279	24,6	3527	1123	31,8
2016	98036	27731	28,3	4443	1750	39,4
2017	118736	29663	25,0	4528	2158	47,7
2018	106150	30513	28,7	6073	3696	60,9
2019	125044	37327	29,9	9566	6330	66,2
2020	123608	38808	31,4	10124	6701	66,2
2021	153954	59667	38,8	18421	14469	78,5
2022	145098	62685	43,2	25464	20171	79,2

Źródło: opracowanie własne na podstawie danych przekazanych z KGP drogą mailową

Liczba stwierdzonych przestępstw (tabela 2) zarówno z art. 286, jak i z art. 287 k.k., podobnie jak w przypadku wszczętych postępowań, wskazuje na rosnący trend w wykorzystaniu nowych technologii w działalności przestępczej. Pokazuje to również powagę problemu oraz potrzebę podejmowania jeszcze bardziej zintensyfikowanych działań profilaktycznych.

Liczba odnotowanych przez policję przestępstw z art. 287 w 2021 i 2022 r., wśród których aż niespełna 80% stanowiły te dotyczące bankowości elektronicznej oraz prób np. wyłudzenia danych logowania, wskazuje, iż należy zrewidować podejście do informowania i edukowania obywateli co do sposobów działania przestępców w tym zakresie.

Tabela 3. Liczba pełnoletnich pokrzywdzonych w związku z wybranymi artykułami k.k.

Rok	Art. 286 § 1–3		%	Art. 287 § 1–2		%
	Wszystkie	Internetowe		Wszystkie	e-bankowość, *phishing*	
2013	50333	13345	26,5	988	–	–
2014	58708	18401	31,3	1453	345	23,7
2015	61838	25388	41,1	2236	735	32,9
2016	60999	22474	36,8	3640	1594	43,8
2017	65036	26860	41,3	3573	1952	54,6
2018	63774	27359	42,9	5406	3488	64,5
2019	77834	33239	42,7	8292	5791	69,8
2020	69971	34814	49,8	9342	6551	70,1
2021	107408	54116	50,4	18188	14377	79,0
2022	105316	57255	54,4	24475	20126	82,2

Źródło: opracowanie własne na podstawie danych przekazanych z KGP drogą mailową

Tabela 4. Liczba niepełnoletnich pokrzywdzonych w związku z wybranymi artykułami k.k.

Rok	Art. 286 § 1–3		%	Art. 287 § 1–2		%
	Wszystkie	Internetowe		Wszystkie	e-bankowość, *phishing*	
2013	222	71	32,0	13	–	–
2014	240	121	50,4	7	1	14,3
2015	272	135	49,6	11	6	54,5
2016	307	162	52,8	29	11	37,9
2017	371	198	53,4	26	15	57,7
2018	369	256	69,4	15	5	33,3
2019	392	284	72,4	78	30	38,5
2020	419	327	78,0	41	25	61,0
2021	785	547	69,7	110	88	80,0
2022	739	540	73,1	244	201	82,4

Źródło: opracowanie własne na podstawie danych przekazanych z KGP drogą mailową

Z przedstawionych danych wynika, że częściej ofiarami przestępstw komputerowych padają osoby pełnoletnie (tabela 3). Związane jest to między innymi z tym, iż posiadają one znacznie większe środki finansowe niż nieletni. Niemniej jednak dane z tabeli 4 wskazują, że osoby niepełnoletnie coraz częściej znajdują się w kręgu zainteresowań cyberprzestępców. Jak można zauważyć, liczba nieletnich, którzy pokrzywdzeni zostali w związku z art. 287 w 2022 r. wzrosła ponad dwukrotnie w porównaniu do roku 2021.

Mimo iż uznać można, że liczba osób pokrzywdzonych zarówno w odniesieniu do art. 286, jak i art. 287 k.k. nie jest duża – ogółem stanowi to niespełna pół procenta obywateli Polski, w perspektywie czasu stanowić może ogromny problem. Wszystko za sprawą rozwoju technologicznego, który w coraz większym stopniu ułatwia cyberprzestępcom ich działalność.

Propozycje działań prewencyjnych wśród osób starszych

Z uwagi na narażenie na działanie cyberprzestępców głównie osób o niskich kompetencjach cyfrowych, często są to osoby 60+, to do nich skierować należy szczególne działania uświadamiające czyhające na nie zagrożenia. Z tego też względu należy zadbać, aby w ten trudny proces zaangażowali się wszyscy, a w szczególności ogólnie pojęte media. Ich rola jest ogromna z uwagi na funkcje, jakie spełniają, wśród których wymienić należy przede wszystkim informacyjną, interpretacyjną czy też edukacyjną[24].

Jednym z przykładów działań zmierzających do uświadomienia i edukowania osób starszych, między innymi z zakresu nowych technologii (w tym bezpieczeństwa cyfrowego), jest podcast realizowany przez Wiktora Niedźwieckiego w Radiu Pogoda. Nosi on tytuł „Technicznie proste w Radiu Pogoda"[25].

Innymi przykładami działań podejmowanych przez media są kampanie społeczne, np. kampania prezesa UOKiK pt.: „Stracisz dane, stracisz pieniądze" (rysunek 1)[26] czy też spot CERT Polska pt.: „Co zrobić, jak dostaniesz podejrzany SMS?" (rysunek 2)[27].

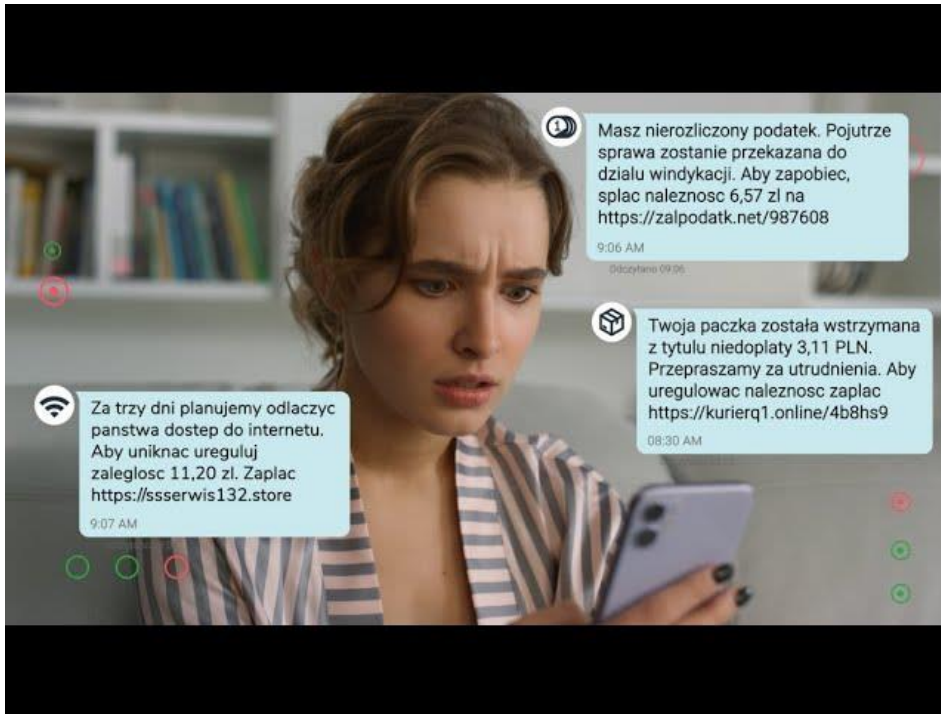
[24] por. A. Kozłowska, *Oddziaływanie mass mediów*, Szkoła Główna Handlowa w Warszawie, Warszawa 2006, s. 69–77; D. McQuail, *Teoria komunikowania masowego*, PWN, Warszawa 2012, s. 111–112.

[25] *Technicznie proste w Radiu Pogoda*, https://radiopogoda.pl/wiktor-niedzicki-technicznie-proste-radio-pogoda-podcasty [dostęp: 3.04.2024].

[26] *Stracisz dane, stracisz pieniądze! – kampania prezesa UOKiK*, https://finanse.uokik.gov.pl/nieautoryzowane-transakcje/stracisz-dane-stracisz-pieniadze-kampania-prezesa-uokik/ [dostęp: 3.04.2024].

[27] NASK PIB, *Co robić, jak dostaniesz podejrzany SMS? CERT Polska i KPRM ostrzegają!*, https://www.youtube.com/watch?v=FZNx15_oURY [dostęp: 3.04.2024].

Rysunek 1. Zrzut ekranu kampanii prezesa UOKiK „Stracisz dane, stracisz pieniądze”



Rysunek 2. Zrzut ekranu spotu CERT Polska „Co zrobić, jak dostaniesz podejrzany SMS?”

Obie te kampanie miały na celu uczulić ludzi na próby wyłudzania ich danych, chociażby w postaci fałszywych SMS-ów czy też maili do złudzenia przypominających takie, które może do nas wysłać jakaś instytucja lub firma (np. z informacją o niezapłaconej fakturze).

Najnowsza kampania, jaką można zobaczyć w telewizji, realizowana jest przez mBank i nosi nazwę „Kurs samoobrony przed cyberoszustami”[28]. Jest to seria siedmiu spotów, z których każdy dotyczy innego rodzaju oszustwa czy ataku. W ramach działań edukacyjnych mBank przygotował również stronę internetową (mbank.pl/samoobronawsieci), na której zamieszczone zostały wszystkie spoty wraz z quizem umożliwiającym sprawdzenie swoich umiejętności radzenia sobie z cyberoszustami.

Wymienione tu kampanie najczęściej wyświetlane są w ramach bloków reklamowych emitowanych w telewizji i radiu. Z tego też względu mogą nie docierać do odbiorców w takim zakresie, jak powinny z uwagi na problem, jakiego dotyczą. Stąd też należy zastanowić się nad innym rozwiązaniem. Jednym z nich może być prezentowanie tych spotów w mediach, ale nie w blokach reklamowych, a osobno w trakcie trwania programów o największej oglądalności, wówczas zwiększy się prawdopodobieństwo, że zostaną obejrzane przez widzów.

Innym pomysłem na dotarcie z informacją do konkretnej grupy odbiorców jest np. umieszczenie kwestii cyberbezpieczeństwa i sposobów działania cyberoszustów jako wątku w popularnych serialach telewizyjnych. Wówczas widzowie, którzy często utożsamiają się z bohaterami, zwrócą uwagę na potencjalne zagrożenie. Można również zrealizować spoty z udziałem aktorów serialowych, którzy nadal wcielając się w kreowanych przez siebie bohaterów, przedstawialiby prawidłowe zachowania w przypadku zaistnienia cyberzagrożenia.

Zakończenie

Rozwój nowoczesnych technologii oprócz ułatwiania funkcjonowania jej użytkownikom wpłynął na zwiększenie się przestępczości. Spowodowane jest to między innymi ułudą anonimowości w sieci Internet, a co za tym idzie, bezkarności. Podobnego zdania jest Z. Majchrzyk, który twierdzi, że „nigdy wcześniej ludzie nie mieli możliwości tak bezkarnie i intensywnie dawać upust własnym frustracjom”[29]. Nie do końca jest to jednak prawdą, ponieważ wszystko, co ro-

[28] *mBank – Samoobrona w sieci mBank,* https://www.mbank.pl/lp2/2023/w1/samoobrona-wsieci/ [dostęp: 3.04.2024].

[29] Z. Majchrzyk, *Cyberprzestępstwa – aktywność poznawcza czy przyjemność* [w:] *Patologie w cyberświecie*, red. S. Bębas, J. Plis, J. Bednarek, Wyższa Szkoła Handlowa w Radomiu, Radom 2012, s. 167.

bimy w świecie cyfrowym, pozostawia ślad. Dzięki temu „wszelkie działania o charakterze przestępczym, prędzej czy później zostaną wykryte, a ich sprawcy mogą zostać ukarani”[30].

Nie ulega wątpliwości, że wyeliminowanie cyberprzestępczości jest niemożliwe. Zwłaszcza że „kreatywność oszustów na wyłudzanie środków finansowych właściwie nie zna granic”[31]. M. Gruchoła również słusznie zauważa, że „obecnie ściganie cyberprzestępstw stało się wyjątkowo trudne. Przyczyniły się do tego szybko rozwijające się technologie informacyjne, coraz większy zasięg Internetu oraz gwałtowny wzrost szybkości wymiany informacji”[32]. Dlatego też należy podejmować odpowiednie działania edukacyjne, najlepiej kierowane do konkretnych grup odbiorców, które będą miały możliwie jak największy zasięg.

Podejmowane przez różne instytucje działania nie do końca wydają się efektywne, zwłaszcza patrząc na rokrocznie rosnące statystyki związane z oszustwami komputerowymi. Z tego też względu należy zastanowić się nad zmianą podejścia do wykorzystania mediów w procesie edukowania społeczeństwa w zakresie cyberprzestępczości.

Zaprezentowane w niniejszym artykule propozycje nowych rozwiązań zapewne nie są idealne i nie rozwiążą w zupełności problemu cyberoszustw. Jednakże mogą okazać się pomocne w ograniczeniu liczby osób pokrzywdzonych.

Bibliografia

Cyberbezpieczeństwo. Zarys wykładu, red. C. Banasiński, Wolters Kluwer Polska, Warszawa 2018.

Cybercrime [w:] *Wikipedia*, 2022.

Czerski W.M., *Cyberprzestępczość wśród nieletnich – charakterystyka zjawiska, jego skala i przeciwdziałanie*, „Dydaktyka Informatyki” 2022, t. 17.

Dennis M.A., *Cybercrime – Spam, steganography, and e-mail hacking | Britannica*, https://www.britannica.com/topic/cybercrime [dostęp: 16.01.2022].

Garwol K., *Polska szkoła w dobie zagrożenia cyberprzestępczością*, „Dydaktyka Informatyki” 2018, t. 13.

Gruchoła M., *Polityka Unii Europejskiej w zakresie cyberprzestępczości* [w:] *Patologie w cyberświecie*, red. S. Bębas, J. Plis, J. Bednarek, Wyższa Szkoła Handlowa w Radomiu, Radom 2012.

Jakubski K.J., *Przestępczość komputerowa – zarys problematyki*, „Prokuratura i Prawo” 1996, nr 12.

[30] W.M. Czerski, *Cyberprzestępczość wśród nieletnich – charakterystyka zjawiska, jego skala i przeciwdziałanie*, „Dydaktyka Informatyki” 2022, t. 17, s. 12.

[31] A. Piecuch, *Szkoła XXI wieku – problemy i wyzwania*, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2019, s. 227.

[32] M. Gruchoła, *Polityka Unii Europejskiej w zakresie cyberprzestępczości* [w:] *Patologie w cyberświecie*, red. S. Bębas, J. Plis, J. Bednarek, Wyższa Szkoła Handlowa w Radomiu, Radom 2012, s. 161.

Jaroszewska I.A., *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, „Kortowski Przegląd Prawniczy", Olsztyn 2017.
Kosiński J., *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015.
Kozak S., *Patologie komunikowania w Internecie: zagrożenia i skutki dla dzieci i młodzieży*, Difin, Warszawa 2011.
Kozłowska A., *Oddziaływanie mass mediów*, Szkoła Główna Handlowa w Warszawie, Warszawa 2006.
Maciejczyk R., *Bankowość elektroniczna – zagrożenia*, „Kwartalnik Policyjny" 2017, nr 4(43).
Majchrzyk Z., *Cyberprzestępstwa – aktywność poznawcza czy przyjemność* [w:] *Patologie w cyberświecie*, red. S. Bębas, J. Plis, J. Bednarek, Wyższa Szkoła Handlowa w Radomiu, Radom 2012.
mBank – Samoobrona w sieci mBank, https://www.mbank.pl/lp2/2023/w1/samoobronawsieci/ [dostęp: 3.04.2024].
McQuail D., *Teoria komunikowania masowego*, PWN, Warszawa 2012.
mObywatel 2.0 – Aplikacja mobilna i serwis dla obywateli, https://info.mobywatel.gov.pl/ [dostęp: 10.03.2024].
NASK PIB, *Co robić, jak dostaniesz podejrzany SMS? CERT Polska i KPRM ostrzegają!*, https://www.youtube.com/watch?v=FZNx15_oURY [dostęp: 3.04. 2024].
Piecuch A., *Szkoła XXI wieku – problemy i wyzwania*, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2019.
Profil zaufany – Portal Gov.pl, https://www.gov.pl/web/profilzaufany [dostęp: 10.03.2024].
Rogowski A., *Phishing*, „Kwartalnik Policyjny" 2017, nr 4(43).
Schjølberg S., *Computers and penal legislation: a study of the legal politics of a new technology*, Universitetsforlaget, Oslo 1983.
Siwicki M., *Cyberprzestępczość*, C.H. Beck, Warszawa 2013.
Siwiecki M., *Oszustwa nigeryjskie – próba klasyfikacji*, „Kwartalnik Policyjny" 2017, nr 4(43).
Stracisz dane, stracisz pieniądze! – kampania prezesa UOKiK, https://finanse.uokik.gov.pl/nieautoryzowane-transakcje/stracisz-dane-stracisz-pieniadze-kampania-prezesa-uokik/ [dostęp: 3.04.2024].
Technicznie proste w Radiu Pogoda, https://radiopogoda.pl/wiktor-niedzicki-technicznie-proste-radio-pogoda-podcasty [dostęp: 3.04.2024].
Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 2021, poz. 2345, 2447).
Vishing, https://www.knf.gov.pl/dla_konsumenta/kampanie_informacyjne/cyberoszustwa_inwestycyjne/schematy_oszustw/vishing?articleId=87578&p_id=18 [dostęp: 29.03.2024].
Warchoł A., *Przestępstwa komputerowe i problemy wojny w cyberprzestrzeni* [w:] *Elementy bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Analiza wybranych systemów*, red. P. Swoboda, A. Żebrowski, Avalon, Kraków 2020.
Wasilewski J., *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, t. 8, nr 15.
Witek K., *Przestępczość komputerowa – aspekty prawne*, „Edukacja – Technika – Informatyka" 2018, t. 24, nr 2.