

DOI: http://dx.doi.org/10.12775/AUNC_PED.2024.002

Wioletta Jachym^{A, C, D, E, G}

Wydział Humanistyczny, Katedra Pedagogiki

Akademia Tarnowska

ORCID: 0000-0002-1153-5727

w_jachym@atar.edu.pl

Natalia Kolman^{A, B, E, F}, Zuzanna Mikulec^{A, B, E, F},

Karolina Nowak^{A, B, E, F}, Daria Zuchowicz^{A, B, E, F},

Kinga Brzeska^{A, B, E, F}, Rozalia Mitoraj^{A, B, E, F},

Paulina Sarad^{A, B, E, F}, Wiktoria Kurtyka^{A, B, E, F}

Studentki kierunku pedagogika przedszkolna
i wczesnoszkolna w Akademii Tarnowskiej

A – przygotowanie badań, B – gromadzenie danych, C – analiza uzyskanych wyników,
D – interpretacja uzyskanych wyników, E – przygotowanie wersji pierwotnej tekstu, F – przegląd
literatury, G – korekta i rewizja tekstu

CO KRYJE SIĘ W SIECI? NEGATYWNE ZACHOWANIA W INTERNECIE

What is Hidden on the Internet? Negative Behavior on the Internet

Streszczenie

Celem artykułu jest przedstawienie zagadnień związanych z negatywnymi zjawiskami w Internecie, których doświadczają jego użytkownicy. W pierwszej części opracowania podjęto próbę charakterystyki cyberprzemocy i phishingu.

Opracowanie zawiera omówienie wskazanych zjawisk oraz prezentację wyników badań empirycznych przeprowadzonych w tym zakresie. Zwrócono uwagę na dwa aspekty – doświadczenie cyberprzemocy w grupie studentów i poziom wiedzy osób biorących udział w badaniach dotyczących zagadnienia phishingu. Wyniki przeprowadzonych badań potwierdzają, że cyberprzemoc jest zjawiskiem powszechnym i przykłady jego wystąpienia są znane w grupie studentów biorących udział w badaniach. Phishing również jest rozpoznawalny w grupie badawczej, ale uczestnicy badania mają zróżnicowaną wiedzę na temat tego, w jaki sposób zapobiegać phishingowi i gdzie się zgłosić w sytuacji jego wystąpienia.

Słowa kluczowe: bezpieczeństwo w Internecie, cyberprzestrzeń, cyberprzemoc, phishing

Abstract

The aim of the article is to present issues related to negative phenomena on the Internet experienced by its users. The first part of the study attempts to characterize cyberbullying and phishing. The study covers a discussion of the indicated phenomena and a presentation of the results based on empirical research conducted in this field. The two following aspects were paid special attention to: the experience of cyberbullying in a group of students and the level of knowledge pertaining to the issue of phishing of people participating in the research. The results of the conducted research confirm that cyberbullying is a common phenomenon and examples of its occurrence are known in the group of students participating in the research. Phishing is also familiar to the group of respondents in the study. However, the knowledge on the subject of how to prevent phishing and where to report it if it occurs varies considerably among the participants.

Key words: Internet safety/security, cyberspace, cyberbullying, phishing

Wprowadzenie

Cyberprzestrzeń stała się dla większości społeczeństwa nierozdzielalnym elementem życia. Dzięki rozwojowi cyfryzacji i popularyzacji urządzeń mobilnych wiele aktywności podejmowanych przez

człowieka przeniesionych zostało do świata wirtualnego. Rzeczywistość ta dała możliwości rozwoju, nauki, komunikacji, realizacji pracy zawodowej, rozrywki, zakupów, e-usług. Rozwój cyberprzestrzeni i wzrost liczby jej użytkowników są związane ze zwiększeniem dostępności do Internetu. Z badań UE dotyczących wykorzystania technologii informacyjno-komunikacyjnych (ICT) w gospodarstwach domowych i przez osoby fizyczne wynika, że liczba ta wciąż rośnie. Według danych Eurostatu za rok 2023 Polska zajmowała pod tym względem 18. miejsce – w naszym kraju dostęp do Internetu posiada 94,19% gospodarstw domowych (Eurostat 2024; zob. tab. 1). Z danych Głównego Urzędu Statystycznego wynika, że w 2023 roku blisko 93% gospodarstw domowych w Polsce miało w domu dostęp do Internetu szerokopasmowego, tj. o 0,2 p. proc. więcej niż przed rokiem (Gumiński 2023, s. 24). Dane te wskazują na ciągły rozwój cyberprzestrzeni.

Tabela 1. Gospodarstwa domowe – poziom dostępu do Internetu

GEO (Labels)	Time 2023	GEO (Labels)	Time 2023
1. Switzerland	100,00	16. Belgium	94,63
2. Luxembourg	99,88	17. Italy	94,19
3. Norway	99,20	18. Poland	94,19
4. Netherlands	98,98	19. Latvia	93,86
5. Finland	98,37	20. Ireland	93,77
6. Spain	97,32	21. Estonia	93,75
7. Denmark	96,81	22. Malta	93,29
8. Sweden	96,54	23. Bulgaria	93,07
9. Hungary	96,39	24. Portugal	93,02
10. Austria	96,09	25. Croatia	92,94
11. Romania	96,04	26. Germany	92,75
12. Slovenia	95,27	27. Lithuania	92,42
13. Slovakia	95,20	28. Cyprus	92,17
14. France	95,14	29. Greece	91,09
15. Czechia	94,70	30. Bosnia and Herzegovina	83,77

Źródło: Eurostat 2024.

W literaturze przedmiotu znajdziemy różne definicje cyberprzestrzeni. W *Wielkim słowniku języka polskiego* cyberprzestrzeń została określona jako „interaktywny, wirtualny świat, utworzony przez komputery połączone w sieci” (Dereń, Polański 2008, s. 120). W encyklopedii komputerowej określono definicję cyberprzestrzeni, przedstawiając jej dwa wyjaśnienia: „1. Zaawansowana, współdzielona sieć rzeczywistości wirtualnej wymyślona przez Williama Gibsona w jego powieści *Neuromancer* z 1982 r. 2. Ogólnoświatowe środowisko sieciowe takie jak Internet, w którym ludzie kontaktują się przez połączone ze sobą komputery. Jego zasadniczą cechą jest to, że umożliwia komunikację niezależnie od fizycznej odległości” (Woodcock 2002, s. 135). Z kolei w *Encyklopedii pedagogicznej XXI wieku* cyberprzestrzeń została opisana jako „zespół zróżnicowanych, multimedialnych i wielozmysłowych informacji, stanowiących alternatywną czasoprzestrzeń” (Pilch 2003, s. 542). Cyberprzestrzeń wzbudza ogromne zainteresowanie badaczy różnych dyscyplin naukowych, skupiając ich uwagę na zaletach tego środowiska, ale także na kwestiach zagrożeń wynikających z jej użytkowania. Niestety aspekty negatywne są coraz częściej dostrzegane, analizowane i omawiane na podstawie wyników prowadzonych badań.

Internet wykorzystywany pierwotnie do słusznych idei, takich jak: komunikacja, praca i nauka, stworzył przestrzeń do rozwoju wielu negatywnych zjawisk, w tym zachowań o charakterze patologicznym, a często także kryminalnym (cyberprzemoc, phishing). Wymienione zagadnienia zostaną bliżej omówione w dalszej części opracowania.

Przegląd literatury – ramy definicyjne

Cyberprzemoc

Cyberprzemoc to coraz powszechniejszy problem, który dotyka osoby w każdym wieku, niezależnie od płci, rasy, pochodzenia czy przekonań. Może przybierać różne formy – od wysyłania obraźliwych wiadomości po poniżanie i zastraszanie w mediach społecznościowych. Cyberprzemoc może mieć poważne konsekwencje dla ofiar, prowadząc

do depresji, lęku, a nawet samobójstwa. W tej części artykułu zostanie bliżej opisane zjawisko cyberprzemocy, jej formy i wpływ na ofiary.

W wielu publikacjach naukowych oraz w debacie publicznej pojęcie cyberprzemocy wyjaśniane jest w kontekście takich terminów jak: bullying w cyberprzestrzeni, cyberbullying, agresja elektroniczna, mobbing elektroniczny. Jest to stosunkowo nowe zjawisko definiowane zwykle jako „forma mobbingu wyrażająca się poprzez media i urządzenia służące komunikacji, jak telefony komórkowe, e-mail oraz Internet (np. portale społecznościowe, strony internetowe i blogi)” (Lizut 2014, s. 87). Nancy E. Willard w swojej książce poświęconej cyberprzemocy i cyberzagrożeniom opisała odmiany tego zjawiska. Jako przykłady wymieniła m.in.:

- flaming: wysyłanie agresywnych wiadomości do konkretnej osoby lub grupy za pośrednictwem komunikatora;
- zastraszanie online: powtarzalne wysyłanie obraźliwych wiadomości e-mailowych lub w innej formie do osoby zastraszanej;
- cyberstalking: zastraszanie online w formie pogroźek;
- dyskredytacja: wysyłanie nieprawdziwych, oszczerczych informacji o określonej osobie do innych lub zamieszczanie takich informacji w Internecie;
- wykluczenie: wykluczenie kogoś z grupy online w brutalny sposób (Willard 2007, s. 5).

Trudno oszacować skalę zjawiska cyberprzemocy. W jednym z ostatnich raportów Amnesty International z 2023 roku przeczytamy, że „w Polsce jedna na dziesięć osób (9,5%) doświadczyła osobiście cyberprzemocy. Dziewięć na dziesięć osób (87% wśród ogółu i 91,1% wśród młodych) spotkało się z nią wielokrotnie. Co ważne, 26,7% młodych osób spotyka się z nią regularnie – przynajmniej dwa razy w miesiącu” (Amnesty International 2024). Wśród wniosków przedstawionych w raporcie Europejskiego Biura Regionalnego Światowej Organizacji Zdrowia (WHO) (Cosma 2024) znajdziemy następujące stwierdzenie: cyberprzemoc niepokojąco rośnie. Jedne z ważniejszych wniosków z badań prowadzonych w Polsce przedstawiają się w następujący sposób:

- około 12% nastolatków stosuje cyberprzemoc wobec innych; sprawcami przemocy są częściej chłopcy niż dziewczęta; najwyższy

odsetek sprawców cyberprzemocy obserwuje się wśród 15-letnich chłopców i 13-letnich dziewcząt;

- 15% nastolatków doświadcza cyberprzemocy; grupą najbardziej narażoną na cyberprzemoc są 13-latk.

Objawy i skutki cyberprzemocy

Osoba doświadczająca cyberprzemocy często nie jest w stanie samodzielnie sobie z nią poradzić. Kluczowa jest postawa świadków zaistnienia formy przemocy, w tym członków rodziny i znajomych. Ofiara cyberprzemocy doświadcza m.in. lęku, poczucia osamotnienia i zagrożenia, obniżenia nastroju i samooceny, frustracji, gniewu, alienacji społecznej. Bardzo poważnym skutkiem bycia ofiarą cyberprzemocy jest depresja, często połączona nawet z myślami samobójczymi (Nowakowski 2018, s. 46). Impulsem, który powinien nas skłonić do pewnych podejrzeń i podjęcia działań zapobiegawczych, są niepokojące objawy zachowania ofiary cyberprzemocy. Mowa tutaj o takich objawach jak: napięcie emocjonalne, skrywany płacz, niska samoocena, wycofanie, skłonność do izolacji, smutek, natręctwa, zachowania kompulsywne, słaba kontrola emocji, wzrost agresji, impulsywność, zmienność nastroju, pogorszenie w kontaktach z rówieśnikami, nieufność, lęki, chęć izolacji, awersja do otoczenia (Szmydt 2015, s. 11). W przypadku dzieci o tym, że dzieje się coś niepokojącego, mogą także świadczyć takie objawy jak: unikanie szkoły, zdenerwowanie, smutek, brak chęci rozmów na temat tego, co robiło z użyciem komputera lub telefonu, nagły brak zainteresowania urządzeniami elektronicznymi, obawa przed pokazywaniem się publicznie (Szulc 2018, ss. 5–6).

Ciekawego zestawienia skutków cyberprzemocy w ujęciu holistycznym w stosunku do ofiary i sprawcy w różnym stopniu i stadium nasilenia dokonała Aldona Rumińska-Szalska (2023, ss. 97–98), przedstawiając skutki przemocy w obszarze psychicznym, fizycznym, społecznym i duchowym. W swoim opracowaniu podkreśliła, że skutki cyberprzemocy dotyczą wielu obszarów funkcjonowania człowieka i mają realny wpływ na rzeczywistość, w której żyjemy.

Profilaktyka cyberprzemocy

W celu minimalizacji skali zjawiska cyberprzemocy ważna jest edukacja społeczeństwa w tym zakresie. Mowa tu nie tylko o edukacji mającej na celu wyjaśnienie, czym jest cyberprzemoc i jakie przybiera formy, jakie mogą być jej skutki, lecz także o edukacji w zakresie odpowiedzialności karnej osób, które ją stosują. Podstawowymi elementami edukacji w tym obszarze mogą być takie zagadnienia jak samokontrola – hamowanie emocji i zachowań agresywnych w sieci oraz empatia – rozumienie perspektywy i poglądów innych osób. Ciekawą propozycją może być zastosowanie treningu uważności – mindfulness – jako techniki pracy z młodzieżą w aspekcie profilaktyki cyberprzemocy (Gregorek 2018, s. 35). Dla wszystkich, którzy chcą edukować użytkowników Internetu, w tym dzieci i młodzież, dostępnych jest wiele publikacji z omówieniem podstawowych zagadnień, a często także z gotowymi scenariuszami zajęć. W opracowaniach tych znajdziemy odpowiedź na pytanie, jak budować świadomość bezpiecznego korzystania z sieci internetowej (Grudzień, Sopyło 2020; Siemieniecka, Skibińska, Majewska 2020; Centralny Dom Technologii, Fundacja Polskiego Funduszu Rozwoju 2020; Fundacja Nie Widać Po Mnie 2022). Materiały te są bogatym zbiorem inspiracji do prowadzenia szeroko rozumianej edukacji w zakresie użytkowania zasobów Internetu.

W związku z ciągłym rozwojem technologii, w tym także jej negatywnych aspektów, wiele instytucji i organizacji przygotowuje kampanie informacyjne, kierowane do różnych odbiorców. W tym miejscu można wskazać strony internetowe takich organizacji jak: Fundacja Dajemy Dzieciom Siłę, NASK – Państwowy Instytut Badawczy, Stowarzyszenie „Miasta w Internecie”, a także rządowy serwis internetowy Ministerstwa Cyfryzacji (pod adresem: <https://www.gov.pl/web/baza-wiedzy/aktualnosci>). Kampanie realizowane przez Fundację Dajemy Dzieciom Siłę mają na celu edukowanie dzieci, młodzieży, rodziców i nauczycieli na temat cyberprzemocy, jak jej przeciwdziałać i gdzie szukać pomocy. Szczegóły kampanii dostępne są na stronie internetowej Fundacji. Ciekawe materiały edukacyjne, szkolenia i konkursy znajdziemy na platformie edukacyjnej Fundacji. Innym przykładem jest kampania Stowarzyszenia SOS Wioski Dziecięce i NASK pod hasłem:

„Przemoc w internecie zostawia niewidzialne rany”. Na stronie kampanii można znaleźć nie tylko informacje o tym, jak rozmawiać z dzieckiem o cyberprzemocy, lecz także wskazówki, jak jej przeciwdziałać. Na stronie internetowej NASK znajdziemy scenariusze skierowane do różnych grup wiekowych, od przedszkolaków, aż po uczniów szkół ponadpodstawowych. W ramach Polskiego Centrum Programu Safer Internet realizowane są trzy projekty: Saferinternet.pl, Pomoc telefoniczna i online, a także Dyżurnet.pl. Na stronie internetowej Centrum warto zaznajomić się z materiałami kampanii informacyjnych i projektów edukacyjnych, w tym m.in. z serwisem <https://sieciaki.pl/>. Pełny dostęp do zasobów serwisu możliwy jest po założeniu darmowego konta. Serwis zawiera takie zasoby jak: kurs interaktywny „Bezpieczny Internet”, słuchowiska, gry, scenariusze lekcji, kreskówki, komiksy, grafiki do pobrania.

Oprócz wyżej wymienionych przykładów istnieje wiele innych kampanii informacyjnych, projektów fundacji i działań profilaktycznych odnoszących się do cyberprzemocy. Więcej informacji na ten temat można znaleźć na stronach internetowych m.in. Fundacji Dzieci Niczyje, Rzecznika Praw Dziecka, a także Ministerstwa Cyfryzacji.

W zakresie profilaktyki cyberprzemocy nie mniej ważnym elementem jest również edukacja w odniesieniu do świadomości prawnej osób pokrzywdzonych i dopuszczających się przestępstw. W Polsce, w aspekcie cyberprzemocy, ochronę prawną zapewniają Kodeks cywilny oraz Kodeks karny. Przejawy internetowej agresji naruszają obowiązujące prawo i mogą zostać zgłoszone na policję, do prokuratury lub do sądu. Są to m.in. zniesławienie/zniewaga, naruszenie wizerunku, stalking, podszywanie się pod kogoś, groźby, włamania. Prawo zapewnia ochronę w tym zakresie poprzez konstrukcję ochrony dóbr osobistych. Dobrami osobistymi są: „zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska” (Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, art. 23). Ściganie sprawcy cyberprzemocy następuje po złożeniu wniosku przez osobę pokrzywdzoną.

W dalszej części zaprezentowano wyciąg artykułów z Kodeksu karnego, które są podstawą do wszczęcia postępowania i wymierzenia

kary osobom dopuszczającym się łamania prawa w zakresie cyberprzestępczości. Są to m.in.:

- 190 k.k. (groźba karalna), 190a k.k. (uporczywe nękanie, podsywanie się);
- 191 k.k. (zmuszenie do określonego działania), 191a k.k. (naruszenie intymności seksualnej, utrwalenie wizerunku nagiej osoby bez jej zgody);
- 212 k.k. (zniesławienie);
- 216 k.k. (zniewaga);
- 267 k.k. (bezprawne uzyskanie informacji, włamanie się do sieci teleinformatycznych);
- 269 k.k. (uszkodzenie danych informatycznych);
- 269a k.k. (zakłócanie systemu komputerowego);
- 287 k.k. (oszustwo komputerowe) (Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny).

Przytoczone wyżej artykuły stanowią wycinek przestępstw określonych w polskim prawie. Nie ulega wątpliwości, że cyberprzestępczość jest jedną z najszybciej rozwijających się przestępczości. Dlatego tak ważne jest edukowanie społeczeństwa już od najwcześniejszych lat, zwłaszcza w zakresie najczęściej występujących przestępstw, do których należy m.in. wyłudzenie informacji wrażliwych – phishing.

Phishing

Na stronie internetowej Komisji Nadzoru Finansowego przeczytamy, że phishing jest „metodą oszustwa, w której przestępca podszywa się pod inną osobę lub organizację w celu wyłudzenia określonych informacji (na przykład danych logowania do bankowości internetowej) lub nakłonienia ofiary do realizacji określonych działań” (Urząd Komisji Nadzoru Finansowego 2024). Europejska Agencja ds. Cyberbezpieczeństwa określa szeroki charakter phishingu i dzieli go na poszczególne rodzaje. Są to: spear-phishing, whaling, smishing oraz vishing. W opracowaniu Agencji znajdziemy następujące wyjaśnienia:

- „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 agendy rządowe;
- 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” (European Union Agency for Cybersecurity 2023; Matacz, Vodičková 2023).

Efektami phishingu może być utrata poufnych danych osobowych i finansowych. Przestępcy dokonują kradzieży tożsamości, oszustw finansowych, a nawet szantażu. Ofiara ataku może stracić dostęp do konta bankowego, konta pocztowego, kont w mediach społecznościowych i innych kont online, stracić pieniądze z konta bankowego, karty kredytowej lub innych kont finansowych. W przypadku ataku phishingowego na firmę skutkiem takich działań mogą być straty finansowe i utrata reputacji.

Powołując się na informacje przedstawione na stronie internetowej policja.pl, można wskazać, że schemat działania przestępców najczęściej przybiera następujące formy:

- otrzymanie wiadomości e-mail, wyglądającej jak wiadomość od banku, często zawierającej link do strony internetowej, która wygląda jak strona banku – po kliknięciu na link i wpisaniu swoich danych do logowania przestępcy mają dostęp do konta bankowego ofiary i mogą ukraść jej pieniądze;
- otrzymanie wiadomości SMS, która może wyglądać jak wiadomość od firmy kurierskiej – ofiara klika na link, podaje swoje dane osobowe i dane karty płatniczej; przestępcy, posiadając dane ofiary, mogą dokonać nieautoryzowanych zakupów na jej karcie;

- podszywanie się pod fałszywe strony firm, np. sklepów internetowych – ofiara kupuje produkt na stronie internetowej, podaje swoje dane osobowe i dane karty płatniczej; przestępcy mają teraz dane ofiary i mogą ukraść jej pieniądze lub wykorzystać je do innych celów.

W atakach phishingowych można wyszczególnić pewne charakterystyczne cechy niezależnie od sposobu komunikacji atakującego z ofiarą:

- oddziaływanie na emocje – manipulacja ofiary poprzez wzbudzanie wstydu lub strachu, gdyż zastraszona osoba może się obawiać zwrócić po pomoc;
- presja czasu – zachęcanie do nadzwyczajnego pośpiechu i podejmowania nieprzemyślanych decyzji;
- atrakcyjność oferty – przekazywanie informacji o niespotykanych nagrodach lub odziedziczonych fortunach, które mają uśpić czujność ofiary;
- podszywanie się pod autorytet lub zaufaną jednostkę – informacja o podejrzanych działaniach na koncie ofiary, podszywanie się pod policję lub bank;
- niepokojąca treść – wiadomości od najważniejszych instytucji lub znanych firm zawierająca błędy gramatyczne lub ortograficzne;
- podejrzane załączniki bądź odnośniki – kluczowy element phishingu to szkodliwy odnośnik do strony internetowej lub plik (Jancelewicz 2022, ss. 81–83).

Cyberprzestępcy dokonują ataków phishingowych z zastosowaniem wyrafinowanych metod działania. Często wykorzystywany jest element zaufania i podszywania się pod instytucje, co pozwala przestępcom na skuteczniejsze przekonanie ofiary ataku do podania wrażliwych informacji. Dlatego tak ważne jest, aby zachować czujność i nie ufać wszystkim wiadomościom, które otrzymujemy. Więcej informacji na temat phishingu i sposobów ochrony przed nim można znaleźć na stronach internetowych: NASK – Państwowy Instytut Badawczy (Cyberprofilaktyka NASK 2024), CERT Polska (2024) lub na stronie serwisu policja.pl (2024).

Badania empiryczne

W tej części artykułu przedstawiono wyniki badań ankietowych, krótkich sond i wywiadów. Badania zostały przeprowadzone przez studentki kierunku pedagogika przedszkolna i wczesnoszkolna Akademii Tarnowskiej. Badania empiryczne przeprowadzono w obrębie zagadnień poruszanych w niniejszym artykule. Były to tematy związane z cyberprzemocą i phishingiem.

Badanie nr 1 – wywiady

Celem badania pierwszego zespołu było zagadnienie cyberprzemocy i próba ustalenia, czy osoby z otoczenia badaczek miały do czynienia z tą formą przemocy. Założono również, że w sytuacji potwierdzenia faktu osobistego zetknięcia się z cyberprzemocą lub wiedzy rozmówców w tym temacie osoby udzielające wywiadu poproszone zostaną o opisanie tych doświadczeń.

Sformułowano następujące problemy badawcze:

- Jaki jest zakres i charakter doświadczeń związanych z cyberprzemocą wśród młodzieży w wieku 16–22 lata?
- Z jakimi formami cyberprzemocy zetknęły się osoby udzielające wywiadu?

Z uwagi na fakt, że badanie miało z założenia przyjąć charakter badania wstępnego, do wywiadu zaproszono tylko kilka osób. W nagraniach uczestniczyło osiem osób. Grupa rozmówców została dobrana w sposób losowy. Były to osoby z otoczenia studentek przeprowadzających wywiad – znajomi lub studenci spotkani na uczelni.

Poniżej przedstawiono transkrypcję nagrań, podczas których rozmówcy zostali zapytani o to, czy spotkali się z cyberprzemocą, oraz poproszeni o podzielenie się swoimi doświadczeniami.

Nagranie nr 1

Czy kiedykolwiek spotkałaś się z formą cyberprzemocy?

Niestety spotkała mnie cyberprzemoc i było to dwa lata temu. Zapisalam się wtedy na zajęcia taneczne i chciałam pokazać swój układ na pewnej popularnej platformie. Po pewnym czasie od wstawienia filmiku dostałam fale negatywnych komentarzy. Było mi bardzo przykro, przez to straciłam motywację i przestałam tańczyć.

A czy ktoś pomógł Ci w tej sytuacji?

Na początku byłam z tym sama, ale po pewnym czasie moi najbliżsi zauważyli, że coś jest nie tak. Oni pomogli mi i jestem im za to bardzo wdzięczna, bo bez nich nie dałabym sobie rady.

Nagranie nr 2

Czy kiedykolwiek spotkałaś się z formą cyberprzemocy?

Mimo iż już jako dziecko miałam pozakładane konta na wielu portalach społecznościowych, nigdy nie spotkała mnie cyberprzemoc. Zawsze uważałam na to, co oglądam, w co gram i jakie osoby obserwuję w Internecie.

Nagranie nr 3

Czy kiedykolwiek spotkałaś się z formą cyberprzemocy?

Tak. Koledzy w ramach żartu włamali się na moje konto, z którego wypisywali do różnych osób według nich bardzo śmieszne komentarze. Nie, to nie były śmieszne komentarze. Były czasem bardzo obleśne i niesmaczne. Dodatkowo na moją główną stronę, na tablicę dodali obrażający jednego z kolegów post. Post szybko został usunięty. Później koledzy zgłosili, że coś takiego rzekomo dodałam. Nauczyciel wziął mnie na rozmowę, gdzie musiałam się tłumaczyć, że to nie jest możliwe, bo wówczas nie byłam dostępna. Nauczyciel uwierzył mi, ale nikt nie poniósł konsekwencji.

Nagranie nr 4

Czy kiedykolwiek spotkałaś się z formą cyberprzemocy?

Ja osobiście nigdy nie byłam ofiarą cyberprzemocy, ale byłam jej świadkiem. Myślę, że w dzisiejszych czasach problem cyberprzemocy jest

zjawiskiem bardzo powszechnym, gdzie spotykamy się z masą przykrych komentarzy pod postami na Facebooku, Instagramie lub na innych portalach społecznościowych. Uważam, że jest to bardzo poważny problem.

Nagranie nr 5

Czy kiedykolwiek spotkałaś się z formą cyberprzemocy?

Mnie osobiście nie spotkała cyberprzemoc, ale na przykładzie mojej kuzynki mogę się wypowiedzieć. Trzy lata temu opublikowała swoje zdjęcie z wakacji na pewnej platformie. Jej rówieśnicy strasznie zaczęli się z niej wyśmiewać w komentarzach, naprawdę okropne rzeczy jej mówili. Moja kuzynka zaczęła wtedy strasznie płakać i było jej bardzo przykro. Gdy to zobaczyłam, poszłam do jej mamy i musiałyśmy jakoś zareagować. Moja ciocia poszła do szkoły i nauczyciele w porę zareagowali i zatrzymali tę falę hejtu.

Nagranie nr 6

Czy kiedykolwiek spotkałaś się z formą cyberprzemocy?

Nigdy jakoś nie zwracałam uwagi na cyberprzemoc, ponieważ nigdy jej nie doświadczyłam i to zjawisko jest dla mnie obce.

Nagranie nr 7

Czy kiedykolwiek spotkałaś się z formą cyberprzemocy?

Ja osobiście nie miałam styczności z cyberprzestępczością, ale moi znajomi się z nią zetknęli. Moja koleżanka miała pewien problem. Poznała przez Internet chłopaka, z którym rozmawiała kilka tygodni. Później chłopak zaczął być nachalny i niegrzeczny, więc stwierdziła, że utnie z nim kontakt i przestanie z nim rozmawiać. Gdy to zrobiła, zaczął wypisywać nieładne rzeczy o niej, trochę ją zastraszać i nękać. Dużo razy nam o tym mówiła i pokazywała, co jej napisał. Zdarzyło się to wiele razy, w końcu zablokowała go faktycznie na Snapchacie i zgłosiła jego konto na aplikacji. Od tej pory miała spokój. Ale faktycznie ten chłopak wypisywał jej bardzo nieprzyjemne rzeczy, zastraszał ją, że ona narobiła mu jakichś nadziei na coś większego, groził, że on się teraz przez nią zabije. Wiadomości, które on pisał, były bardzo nieprzyjemne i bardzo groźne.

Nagranie nr 8

Czy kiedykolwiek spotkałeś się z formą cyberprzemocy?

Miałem styczność z cyberprzemocą. Było to jakieś kilka lat temu, gdy byłem bardziej aktywny w mediach społecznościowych i wtedy zacząłem otrzymywać obraźliwe wiadomości od ludzi, których totalnie nie znałem. Atakowali mnie z powodu moich pasji i moich poglądów. Te wiadomości były pełne obelg, gróźb, agresji. Było to niekomfortowe, dość przykre doświadczenie, które sprawiło, że znacznie zmniejszyłem swoją aktywność w mediach. Osoby, które zastosowały cyberprzemoc, wykorzystwały anonimowość w Internecie, nie mogłem ich nigdzie znaleźć i mogli wyrazić swoje niezadowolenie i nienawiść do mnie w sposób, w który nie daliby rady w rzeczywistości. Otrzymałem obraźliwe komentarze pod moimi postami w mediach społecznościowych, jak i prywatne wiadomości, które były pełne gróźb i obelg. Nie byłem jedyną osobą, która doświadczyła w moim otoczeniu cyberprzemocy. Wśród moich kolegów i znajomych również zdarzały się podobne przypadki. Niestety cyberprzemoc jest coraz bardziej powszechna i może dotyczyć każdego, niezależnie od wieku, płci czy przekonań.

Wnioski z badania nr 1

1. Cyberprzemoc jest powszechnym problemem, który może dotknąć każdego. Na osiem przeprowadzonych wywiadów trzy osoby doświadczyły cyberprzemocy osobiście, a dwoje rozmówców było jej świadkami.
2. Ofiarami cyberprzemocy mogą być zarówno dzieci, jak i dorośli, niezależnie od płci czy przekonań.
3. Najczęstszymi formami cyberprzemocy są obraźliwe komentarze, groźby i nękanie w mediach społecznościowych.
4. Anonimowość w Internecie ułatwia sprawcom cyberprzemocy krzywdzenie ofiar.

Badanie nr 2 – ankieta

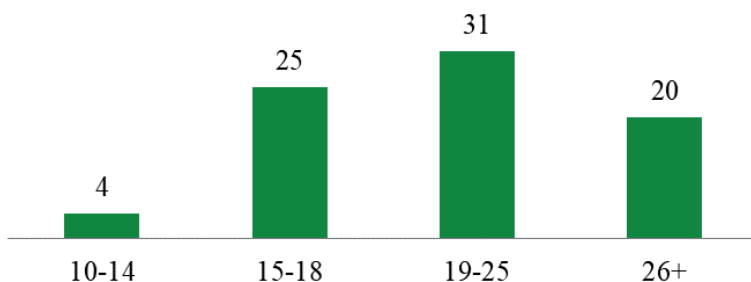
Celem badania drugiej grupy studentek było zagadnienie phishingu. Głównym problemem badawczym było ustalenie poziomu wiedzy respondentów biorących udział w badaniu na temat phishingu.

Sformułowano następujące problemy szczegółowe:

- Jaki jest poziom wiedzy osób biorących udział w ankiecie na temat ataków phishingowych i ich rozpoznawania?
- Czy osoby biorące udział w badaniu posiadają wiedzę na temat tego, gdzie mogą zgłosić ewentualne próby phishingu lub atak phishingowy?

Badanie zostało przeprowadzone na podstawie krótkiej ankiety. Formularz składał się z metryczki, w której zapytano respondentów o wiek i płeć, oraz z czterech pytań zamkniętych i jednego pytania otwartego.

W badaniu wzięło udział 80 osób. Średnia wieku respondentów wynosiła 20 lat, w przedziale od 10 do 28 lat. W grupie tej było 66% kobiet oraz 34% mężczyzn. Struktura wieku respondentów wraz z podaniem ich liczby została przedstawiona na wykresie 1. Dobór respondentów był losowy.

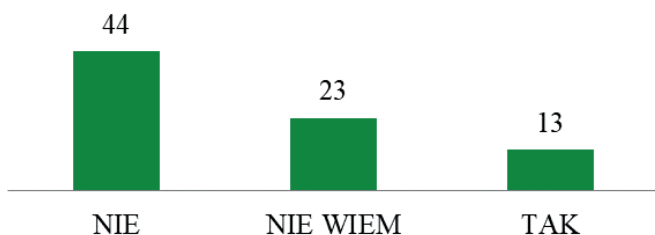


Wykres 1. Struktura wieku respondentów

Źródło: opracowanie własne na podstawie badań.

Omówienie wyników badań

Uwaga zespołu badaczek skierowana została na zagadnienie phishingu. Ankietowani zostali poproszeni o udzielenie odpowiedzi na cztery zasadnicze pytania. Pierwsze z pytań brzmiało: *Czy kiedykolwiek spotkałeś/aś się ze zjawiskiem phishingu?*. Odpowiedzi na to pytanie były zróżnicowane – 55% badanych udzieliło odpowiedzi (nie), 16% badanych udzieliło odpowiedzi (tak), pozostałe osoby, tj. 29%, nie potrafiło udzielić jednoznacznej odpowiedzi i tym samym wskazało na odpowiedź (nie wiem). Wyniki liczbowe w tym zakresie zostały przedstawione na wykresie 2.



Wykres 2. Odpowiedzi na pytanie:
Czy kiedykolwiek spotkałeś/aś się ze zjawiskiem phishingu?

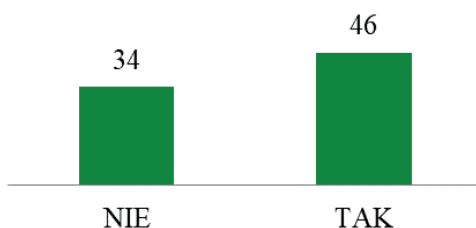
Źródło: opracowanie własne na podstawie badań.

Po udzieleniu odpowiedzi na pierwsze pytanie osobom, które nie posiadały wiedzy na temat tego, czym jest phishing, wyjaśniono to pojęcie. Do osób, które znały to zjawisko, skierowano prośbę o wyjaśnienie, jak rozumieją ten termin i czy mogą podać przykłady phishingu, z którymi się spotkały. Wśród odpowiedzi respondentów znalazły się następujące wyjaśnienia:

- *Fałszywe ogłoszenia o pracę;*
- *Kradzież danych logowania i wyłudzenie przez konto na portalu społecznościowym Facebook;*
- *Ktoś podawał się za pracownika banku;*

- Mężczyzna przedstawił się jako ktoś (nie pamiętam kto dokładnie) i wyłudził pieniądze od mojej cioci w podeszłym wieku;
- Osoba podszyła się pod popularną firmę kurierską, wysyłając link do strony wyglądającej tuzząco podobnie jak strona owej firmy;
- Otrzymanie maila z próbą phishingu i prośbą o wejście w dany link/zatłącznik;
- Po dodaniu ogłoszenia na portalu OLX dostałam wiadomość SMS, że produkt przeze mnie wystawiony został zakupiony. W smsie był link do strony, gdzie miałam się zalogować teoretycznie w celu podania danych swojego konta, aby otrzymać płatność za produkt oraz etykietę na paczkę;
- Próba wyłudzenia pieniędzy;
- Próbný phishing w firmie;
- Wyłudzenia danych do karty kredytowej;
- Zadzwońił do mnie mężczyzna zza wschodniej granicy. Przedstawił się, że jest pracownikiem banku i że wykryto nietypowy ruch na moim koncie. Wysłał mi fałszywe wiadomości, które miały rzekomo potwierdzić to, co on mówi. Podejrzewałem, że jest to oszust, więc rozłączyłem się i zadzwoniłem do banku zapytać się, jak wygląda sytuacja z moim kontem. Okazało się, że nic się z moim kontem nie dzieje, a numer, z którego dzwonił ten mężczyzna, nie należy do banku.

W dalszej części badania respondenci odpowiedzieli na pytanie: *Czy wiesz, gdzie należy się zgłosić w sytuacji wystąpienia phishingu?*. Tylko 58% respondentów posiadało taką wiedzę, natomiast 42% badanych nie wiedziało, gdzie należy zgłosić się po pomoc w takiej sytuacji. Wyniki odpowiedzi na to pytanie zostały zaprezentowane na wykresie 3.

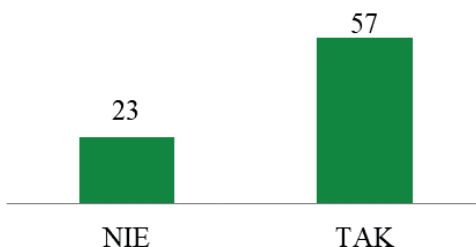


Wykres 3. Odpowiedzi na pytanie:

Czy wiesz, gdzie należy się zgłosić w sytuacji wystąpienia phishingu?

Źródło: opracowanie własne na podstawie badań.

W ostatniej części pytań ankietowych zapytano respondentów o ich dodatkową wiedzę na temat phishingu. Sformułowano pytanie: *Czy wiesz, po czym podejrzewać, że możesz być ofiarą wyłudzenia danych?*. Odpowiedzi respondentów na to pytanie również były zróżnicowane. Tylko 71% ankietowanych wskazało na odpowiedź (tak), pozostałe osoby udzieliły odpowiedzi (nie). Szczegółowe dane przedstawiono na wykresie poniżej.

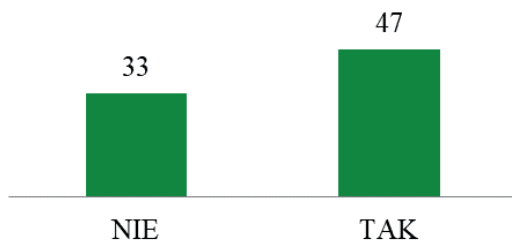


Wykres 4. Odpowiedzi na pytanie:

Czy wiesz, po czym podejrzewać, że możesz być ofiarą wyłudzenia danych?

Źródło: opracowanie własne na podstawie badań.

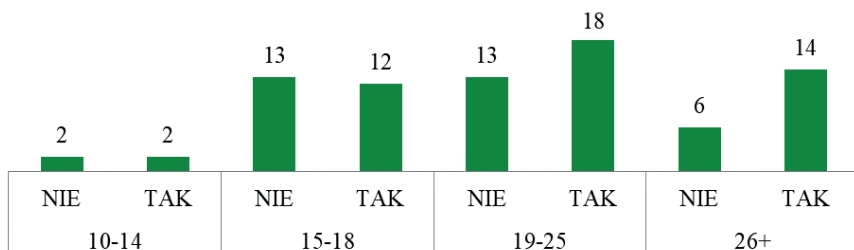
Na zakończenie badań ankietowych zadano pytanie o następującej treści: *Czy posiadasz wiedzę o tym, jak zapobiegać zjawisku phishingu?* Odpowiedzi na to pytanie kształtowały się w sposób następujący: 59% respondentów zadeklarowało, że posiada taką wiedzę, natomiast 41% biorących udział w badaniu zaznaczyło, że brakuje im takiej wiedzy. Dane w tym zakresie przedstawia wykres 5.



Wykres 5. Odpowiedzi na pytanie:
Czy posiadasz wiedzę o tym, jak zapobiegać zjawisku phishingu?

Źródło: opracowanie własne na podstawie badań.

Rozpatrując wyniki badań, przeprowadzono dodatkową analizę danych, zestawiając strukturę wieku respondentów z odpowiedziami na wybrane pytania. W ten sposób uzyskano wyniki, które obrazowały wiedzę respondentów na temat tego, gdzie należy zgłosić się po pomoc w sytuacji zauważenia próby phishingu lub gdy staniemy się ofiarą phishingu. Na podstawie danych przedstawionych na wykresie 7 można sformułować wniosek, że podwyższoną wiedzą w tym zakresie charakteryzują się osoby w grupie wiekowej 19–25 lat. W grupie osób młodszych, tj. grupa 15–18 lat, odpowiedzi są zróżnicowane – 52% osób w tej grupie nie posiada takiej wiedzy. Struktura rozkładu odpowiedzi wskazuje także, że wiedzą w tym zakresie charakteryzują się również osoby z grupy wiekowej 26–28 lat – 70% respondentów potwierdziło posiadanie wiedzy w tym zakresie.



Wykres 6. Struktura odpowiedzi z uwzględnieniem wieku respondentów na pytanie: *Czy wiesz, gdzie zgłosić się po pomoc w sytuacji phishingu?*

Źródło: opracowanie własne na podstawie badań.

Dokonano również analizy, porównując liczbę i strukturę odpowiedzi oraz zestawiając wyniki z dwóch pytań: *Czy kiedykolwiek spotkałeś/aś się ze zjawiskiem phishingu?* oraz *Czy wiesz, gdzie zgłosić się po pomoc w takich sytuacjach?*. Przedstawiona poniżej tabela obrazuje interesujące wyniki. Odpowiedzi osób, które nie spotkały się z phishingiem, były zróżnicowane: 43% osób nie wie, gdzie należy się zgłosić po pomoc, 57% osób posiada taką wiedzę. Zauważalną różnicę odnotowano przy zestawieniu odpowiedzi osób, które nie potrafiły jednoznacznie udzielić odpowiedzi na pytanie, czy spotkały się z phishingiem. W tym przypadku proporcje są zauważalne: 61% osób deklaruje, że nie wie, gdzie należy się zgłosić po pomoc, 39% osób posiada taką wiedzę. Odwrotna sytuacja występuje w przypadku osób, które spotkały się ze zjawiskiem phishingu – aż 92% osób potwierdziło posiadanie wiedzy w tym zakresie.

Tabela 2. Struktura odpowiedzi z uwzględnieniem wiedzy respondentów na temat źródeł pomocy pokrzywdzonym phishingiem

Czy kiedykolwiek spotkałeś/aś się ze zjawiskiem phishingu?	Czy wiesz, gdzie zgłosić się po pomoc w takich sytuacjach?	
	nie wiem, gdzie zgłosić się po pomoc	wiem, gdzie zgłosić się po pomoc
Nie	19	25
Nie wiem	14	9
Tak	1	12
Suma końcowa	34	46

Źródło: opracowanie własne na podstawie badań.

Wnioski z badania nr 2

1. W badaniu dotyczącym phishingu, przeprowadzonym wśród 80 osób, tylko 16% respondentów stwierdziło, że spotkało się osobiście z zagrożeniem phishingu, 55% osób zaprzeczyło, że miały do czynienia z phishingiem, a 29% nie potrafiło jednoznacznie odpowiedzieć.
2. Wiedza na temat postępowania w przypadku phishingu była zróżnicowana: 58% respondentów wiedziało, gdzie zgłosić takie incydenty, natomiast 42% nie miało tej wiedzy, przy czym osoby w wieku 19–25 lat i 26–28 lat wykazywały się większą świadomością w tym zakresie.
3. Na pytanie o umiejętność rozpoznawania phishingu 71% respondentów odpowiedziało twierdząco, a 59% zadeklarowało posiadanie wiedzy na temat zapobiegania phishingowi, co oznacza, że 41% badanych brakowało takiej wiedzy.
4. Analiza wyników wykazała, że osoby, które miały doświadczenie z phishingiem, w znacznie większym stopniu (92%) wiedziały, gdzie zgłosić się po pomoc, w porównaniu z osobami, które nie miały takiego doświadczenia (57%) lub nie były pewne (39%).

Badanie nr 3 – sonda

Tematykę phishingu zbadała również trzecia grupa studentek. Badanie zostało przeprowadzone z zastosowaniem techniki sondy, czyli krótkiego wywiadu. Sondaż przeprowadzono z osobami pełnoletnimi, mieszkańcami miejscowości Szczepanów i Mokrzyńska. Grupa udzielająca odpowiedzi liczyła 37 osób – 17 kobiet, 20 mężczyzn. Celem było zbadanie poziomu świadomości mieszkańców na temat zagrożenia phishingiem w Internecie. Każdej z osób zadano pięć pytań. Treść pytań i wyniki badań przedstawiono poniżej w formie tabelarycznej.

Tabela 3. Wyniki sondy

Pytanie	Odpowiedź TAK	Odpowiedź NIE
<i>Czy wiesz, co to jest phishing?</i> (osoby, które nie znały zjawiska, zostały zapoznane z tematem phishingu)	32 (86%)	5 (14%)
<i>Czy widziałeś/aś kiedyś w Internecie przykłady phishingu?</i>	20 (54%)	17 (46%)
<i>Czy osobiście doświadczyłeś/aś wyłudzenia internetowego?</i>	8 (22%)	29 (78%)
<i>Czy słyszałeś/aś, że Twój znajomy spotkał się z phishingiem?</i>	13 (35%)	24 (65%)
<i>Czy wiesz, co robić w przypadkach, kiedy zostaniesz ofiarą phishingu?</i> (osoba, która nie miała świadomości, jak postępować w takich przypadkach, została poinformowana o procedurze postępowania)	36 (97%)	1 (3%)

Źródło: opracowanie własne na podstawie badań.

Wnioski z badania nr 3

- Większość respondentów zdobywała wiedzę na temat phishingu z różnych źródeł, głównie z Internetu (artykuły, poradniki, strony internetowe), spotkań informacyjnych i kampanii edukacyjnych organizowanych przez instytucje publiczne lub firmy oraz z doświadczeń własnych lub znajomych, którzy byli ofiarami ataków phishingowych.

2. Większość ankietowanych ma świadomość zagrożenia phishingiem, istnieje jednak znacząca grupa osób, która nie jest wystarczająco zorientowana w tym temacie lub nie miała bezpośredniego doświadczenia z atakami phishingowymi.
3. Wyniki badania sugerują konieczność dalszych działań edukacyjnych i promowania bezpiecznych praktyk w zakresie korzystania z Internetu. Takie działania mogą się przyczynić do zwiększenia świadomości społecznej na temat zagrożenia phishingiem i sposobów ochrony przed nim.

Dyskusja i podsumowanie

W dobie powszechnego rozwoju Internetu każdy użytkownik sieci narażony jest na różnego rodzaju zagrożenia cybernetyczne, w tym różne formy cyberprzemocy i ataki phishingowe, mające na celu wyłudzenie danych osobowych. Wyniki przeprowadzonych badań potwierdziły, że najczęstszymi formami cyberprzemocy, z którymi spotkali się respondenci biorący udział w badaniach, były obraźliwe komentarze i groźby wyrażane przeważnie w mediach społecznościowych. Forma agresji słownej wyrażana jest najczęściej przez osoby młode, w wieku dojrzewania. Najbardziej powszechną formą agresji słownej jest poniżanie i wyśmiewanie. Otrzymane wyniki są zgodne z wynikami innych autorów, którzy podejmowali badania w tym temacie z udziałem dzieci, młodzieży i młodych dorosłych (Wędzińska 2023; Pyżalski, Plichta, Szuster, Barlińska 2022; Frankowiak 2020). Podobne wyniki badań znajdują się także w Raporcie z ogólnopolskiego badania uczniów i rodziców. Raport przygotowany przez NASK – Państwowy Instytut Badawczy ujawnia, że niemal połowa młodych ludzi spotyka się w Internecie z atakami werbalnymi i wyzywaniem (44,6%), a co trzeci nastolatek zetknął się z ośmieszaniem (33,2%) i poniżaniem (29,6%). Badani potwierdzili, że dużym problemem w sieci jest mowa nienawiści, a problem ten potęguje anonimowość w Internecie i poczucie bezkarności (NASK 2023). Ten sam fakt podkreślili rozmówcy wywiadów, które były częścią badań opisanych w niniejszym artykule.

Temat cyberbezpieczeństwa z roku na rok zyskuje na popularności. Wynika to z faktu, że coraz więcej czynności życia codziennego realizowanych jest za pomocą technologii. Internet wykorzystywany jest do pracy i nauki, ale także do załatwiania spraw urzędowych, dokonywania zakupów i płatności. Specjaliści z zakresu cyberbezpieczeństwa podkreślają, że największym zagrożeniem w przestrzeni cyfrowej jest phishing. Jak wynika z badania „Postawy Polaków wobec cyberbezpieczeństwa” (KPMG 2024), przede wszystkim boimy się wyłudzenia danych osobowych i wiążącej się z tym kradzieży pieniędzy, a także przywłaszczenia tożsamości. W badaniu KPMG uczestniczyło 100 polskich przedsiębiorstw, obejmujących zarówno duże, średnie, jak i małe firmy, reprezentowane przez osoby zajmujące się zagadnieniami bezpieczeństwa informacji. Wśród cyberzagrożeń stanowiących największe ryzyko dla organizacji najczęściej wymieniano ryzyko wyłudzenia danych uwierzytelniających (phishing). W pięciostopniowej skali 21% badanych wskazało, że ryzyko to jest na najwyższym poziomie. Z podobnymi przykładami phishingu spotkali się również respondenci biorący udział w ankiecie i krótkiej sondzie, której wyniki przedstawiono we wcześniejszej części opracowania. Z badania SMSAPI (2024) wynika, że co drugi ankietowany (53,7%) otrzymał podejrzane treści, np. niespodziewane ponaglenie zapłaty, prośbę o dopłatę czy próby wyłudzenia danych lub podszywanie się pod instytucję, bank, firmę. Osoby biorące udział w badaniach opisywanych w niniejszym opracowaniu również wskazały, że według nich najczęstsze formy phishingu, z którymi się spotkali, to próby wyłudzenia danych i podszywanie się pod banki, platformy sprzedażowe, firmy kurierskie. Jednocześnie ankietowani podkreślili także potrzebę wzmocnienia edukacji i świadomości problemu. Wynika to z faktu, że liczba ataków phishingowych rośnie, przybierają one coraz bardziej wyrafinowane formy działania i trudno jednoznacznie zidentyfikować fałszywe informacje. W raporcie pt. „Dane osobowe – czy wiemy, jak je chronić” (ChronPESEL.pl, Krajowy Rejestr Długów BIG SA 2023), przygotowanym pod patronatem Urzędu Ochrony Danych Osobowych, możemy przeczytać, że zaufanie do swojej wiedzy i świadomości dotyczącej zabezpieczenia własnych danych osobowych maleje wśród różnych grup wiekowych. Badanie zostało przeprowadzone na reprezentatywnej grupie

1007 osób. W raporcie przeczytamy, że zauważalnie spadł odsetek tych, którzy są absolutnie pewni, że nie dadzą się nabrać oszustom. Deklaruje to 18,5% ankietowanych, o ponad 3% mniej niż przed rokiem. Jest to kolejny argument i potwierdzenie potrzeby edukacji w zakresie cyberbezpieczeństwa.

Zjawiska opisane w artykule, takie jak cyberprzemoc i phishing, stanowią istotne problemy współczesnego cyfrowego świata, które wymagają uwagi i podejmowania skutecznych działań prewencyjnych. Cyberprzemoc, rozumiana jako różnego rodzaju formy agresji w Internecie, jest obecnie bardzo rozpowszechniona. Wyniki przywołanych raportów i badań potwierdzają ten fakt. Doświadczenie cyberprzemocy może prowadzić do wielu poważnych konsekwencji psychologicznych, jak depresja, lęk czy nawet myśli samobójcze. W artykule zwrócono uwagę na potrzebę edukowania społeczeństwa na temat cyberprzemocy i phishingu. Kluczowe w tym zakresie jest nie tylko informowanie o samych zjawiskach, lecz także edukowanie użytkowników sieci w zakresie odpowiedzialności korzystania z Internetu, rozpoznawania zagrożeń, sposobów radzenia sobie z nimi oraz odpowiedzialności prawnej za wyrządzone krzywdy. Edukacja ta powinna obejmować wszystkie grupy wiekowe, w tym dzieci, młodzież i osoby dorosłe, gdyż każdy może stać się potencjalną ofiarą cyberprzemocy.

Na zakończenie warto podkreślić znaczenie kampanii informacyjnych i inicjatyw społecznych podejmowanych przez różne organizacje rządowe i pozarządowe. Działania tego rodzaju zwiększają świadomość, promują bezpieczne praktyki w Internecie i proponują formy wsparcia dla ofiar cyberprzemocy i phishingu. Autorki opracowania zaznaczają, że konieczne są dalsze badania i monitorowanie zjawisk związanych z negatywnymi zachowaniami w Internecie. Dzięki temu możliwe będzie lepsze zrozumienie dynamiki tych zjawisk oraz opracowanie skuteczniejszych mechanizmów zapobiegania im.

Bibliografia:

- Amnesty International. *Cyberprzemoc krzywdzi naprawdę*. 2024. <https://www.amnesty.org.pl/badania-prawie-co-piata-mloda-dziewczynyna-doswiadczyla-cyberprzemocy/> (dostęp: 26.05.2024).
- Centralny Dom Technologii, Fundacja Polskiego Funduszu Rozwoju. *Cyberbezpieczni. Scenariusze lekcji o cyberbezpieczeństwie*. 2022. https://fundacjapfr.pl/dam/jcr:4d1306c4-9941-48f7-8b084c1c13bcf2cc/Publikacja_Scenariusze%20lekcji_Cyberbezpieczni_online.pdf (dostęp: 19.08.2024).
- CERT Polska. *(Nie)bezpieczne płatności*. 2024. <https://cert.pl/baza-wiedzy/niebezpieczne-platnosci/> (dostęp: 1.06.2024).
- ChronPESEL.pl, Krajowy Rejestr Długów BIG SA. *Dane osobowe – czy wiemy, jak je chronić?*. 2023. <https://uodo.gov.pl/pl/file/4378> (dostęp: 19.08.2024).
- Cosma, A., Molcho, M., Pickett, W. *A focus on adolescent peer violence and bullying in Europe, central Asia and Canada. Health Behaviour in School-aged Children international report from the 2021/2022 survey*. World Health Organization. Regional Office for Europe 2024. <https://iris.who.int/handle/10665/376323> (dostęp: 19.08.2024).
- Cyberprofilaktyka NASK. *Phishing – czym jest i jak nie dać się złowić oszustom*. 2024. https://cyberprofilaktyka.pl/blog/phishing--czym-jest-i-jak-nie-dac-sie-zlowic-oszustom_i24.html (dostęp: 1.06.2024).
- Dereń, E., Polański, E. „Cyberprzestrzeń”. W: *Wielki słownik języka polskiego*, red. E. Polański, 120. Kraków: Krakowskie Wydawnictwo Naukowe, 2008.
- European Union Agency for Cybersecurity. *ENISA Threat Landscape 2023*. Ateny: European Union Agency for Cybersecurity (ENISA), 2023.
- Eurostat. *Households – level of internet access*. 2024. <https://ec.europa.eu/eurostat/en/web/main/data/database> (dostęp: 1.06.2024).
- Frakowiak, J. „Agresja werbalna w kontekście innych zachowań problemowych adolescentów”. *Kwartalnik Naukowy Fides et Ratio* 42(2) (2020): 445–454.
- Fundacja Nie Widać Po Mnie. *Narzędziownik dla nauczyciela. Czyli co warto wiedzieć o uzależnieniach behawioralnych*. 2022. <https://niewidacpomnie.org/wp-content/uploads/2022/11/NWPM-dla-nauczycieli.pdf> (dostęp: 19.08.2024).
- Gregorek, A. „Mindfulness – trening uważności wśród dzieci i młodzieży w profilaktyce cyberprzemocy”. *Problemy Opiekuńczo-Wychowawcze* 1 (2018): 30–38.

- Grudzień, M., Sopyło, M. *Bezpieczne i odpowiedzialne korzystanie z zasobów sieci. Internet a prawa autorskie*. Warszawa: Ośrodek Rozwoju Edukacji, 2020.
- Gumiński, M., Guzowski, W., Huet, M., Juszczak, K., Kwiatkowska, M., Mor-dan, P., Orczykowska, M. *Społeczeństwo informacyjne w Polsce w 2023 r.* Warszawa–Szczecin: Główny Urząd Statystyczny, 2023.
- Jancelewicz, J. „Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych”. *Trzeci Sektor* 3–4 (2022): 79–88.
- KPMG. *Barometr cyberbezpieczeństwa. Na fali czy w labiryncie regulacji?* 2024. <https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2024/02/pl-Raport-KPMG-w-Polsce-Barometr-cyberbezpiecze%C5%84stwa-2024.pdf> (dostęp: 19.08.2024).
- Lizut, J. *Zagrożenia cyberprzestrzeni*. Warszawa: Wyższa Szkoła Pedagogiczna im. Janusza Korczaka w Warszawie, 2014.
- Matacz, M., Vodičková, W. „Zjawisko phishingu w Polsce”. *De Securitate et Defensione. O Bezpieczeństwie i Obronności* 9(1) (2023): 110–122.
- NASK. *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców*. 2023. <https://www.nask.pl/download/30/4830/ThinkstatRAPORTnastolatki-30ONLINE.pdf> (dostęp: 19.08.2024).
- Nowakowski, K. „Szkodliwość cyberprzemocy w ocenie młodzieży”. *Problemy Opiekuńczo-Wychowawcze* 572(7) (2018): 44–51.
- Pilch, J. „Cyberprzestrzeń”. W: *Encyklopedia pedagogiczna XXI wieku*, t. 1, red. T. Pilch, 542. Warszawa: Żak, 2003.
- Policja.pl. *Top 5 najczęstszych technik phishingowych*. 2024. <https://policja.pl/pol/aktualnosci/212455,Top-5-najczestszych-technik-phishingowych.html> (dostęp: 1.06.2024).
- Pyżalski, J., Plichta, P., Szuster, A., Barlińska, J. 2022. „Cyberbullying Characteristics and Prevention-What Can We Learn from Narratives Provided by Adolescents and Their Teachers?”. *Int J Environ Res Public Health* 19(18): 11589. <https://doi.org/10.3390/ijerph191811589>.
- Rumińska-Szalska, A. „Nauczyciel, uczeń i rodzic w obliczu zjawiska cyberprzemocy rówieśniczej – analiza problemu, profilaktyka, wyzwania”. *Annales Universitatis Mariae Curie-Skłodowska, sectio J – Paedagogia-Psychologia* 36(2) (2023): 89–107.
- Siemieniecka, D., Skibińska, M., Majewska, K. *Cyberagresja. Zjawisko, skutki, zapobieganie*. Toruń: Wydawnictwo Naukowe UMK, 2020.
- SMSAPI. *Bezpieczeństwo cyfrowe Polaków. Oszustwa internetowe i zagrożenia komunikacji mobilnej. Jak bronić się przed oszustwami internetowymi?* 2024.

<https://samorząd.gov.pl/attachment/e187ecd5-d713-4fc8-b02d-ec30641f51c9> (dostęp: 19.08.2024).

Szmydt, B. *Chrońmy młodość w Sieci. Program na rzecz bezpiecznego korzystania z Internetu przez młodzież*. Stalowa Wola: Stowarzyszenie Ruchu Pomocy Psychologicznej INTEGRACJA, 2015.

Szulc, M. „Psychologiczne uwarunkowania, konsekwencje i przeciwdziałanie zjawisku cyberprzemocy”. *Wychowanie na co Dzień* 5–6 (2018): 3–9.

Urząd Komisji Nadzoru Finansowego. *Phishing*. 2024. <https://cebrf.knf.gov.pl/encyklopedia/hasla/385-definicje/818-phishing> (dostęp: 1.06.2024).

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny. Dz.U. z 2023 r. poz. 1610.

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny. Dz.U. z 2024 r. poz. 17.

Wędzińska, M. „Gen Z a cyberbullying – charakterystyka problemu cyberprzemocy w pokoleniu Z”. *Rocznik Towarzystwa Naukowego Płockiego* 15 (2023): 467–489.

Willard, N. E. *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Champaign: Research Press, 2007.

Woodcock, J. „Cyberprzestrzeń”. W: *Microsoft. Encyklopedia komputerowa*, red. J. Woodcock, 135. Warszawa: MIKOM. Klub dla Ciebie, 2002.