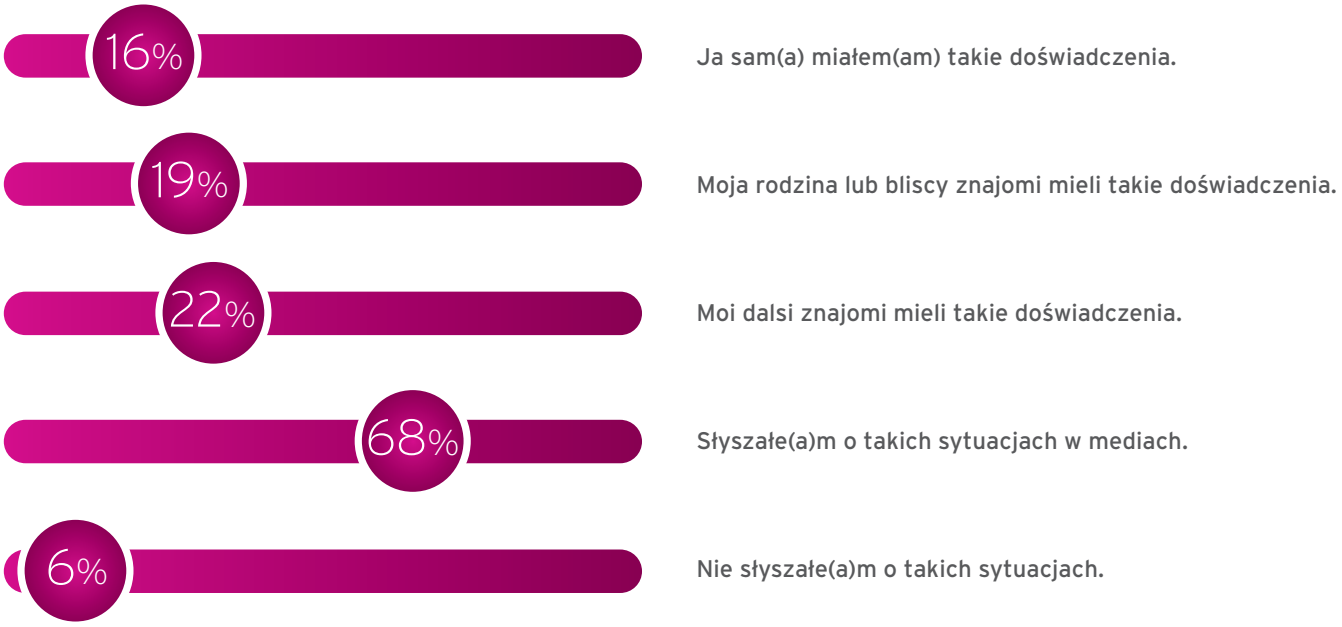
ZŁAPANI W SIEĆ – JAK POLACY RADZĄ SOBIE W CYBERRZECZYWISTOŚCI

Fundacja Kronenberga
citi handlowy
inspiracja do działania

ZDAJEMY SOBIE SPRAWĘ Z CYBERZAGROŻEŃ



Cyberbezpieczeństwo użytkowników banków, raport przygotowany przez IQS na zlecenie Fundacji Kronenberga Citi Handlowy, marzec 2020, Próba, N=1111 w wieku 15-55 lat.

Pandemia zamknęła nas w domach i wymusiła przeniesienie wielu naszych aktywności do sieci. Jak wynika z lipcowego badania IMAS International zleconego przez KRD[1] ponad połowa z nas (54,3%) w czasie pandemii spędza więcej czasu online. Szczególnie dotyczy to czasu wolnego – poza pracą pozostajemy w sieci najczęściej 2–4 godziny dłużej niż przed pandemią.

Zmieniają się też nasze nawyki. Badanie KMPG[2] pokazało, że zdecydowana większość Polaków (71%), mając do kupienia produkty inne niż spożywcze rezygnuje z wizyty w sklepie stacjonarnym i dokonuje zakupu online. Co trzeci z nas (34%) zaczął kupować w sieci produkty, które wcześniej nabywał wyłącznie stacjonarnie. Funkcjonowanie w internecie na pewno pozwala unikać ryzyka zakażenia, jednak naraża nas na liczne zagrożenia czyhające w rzeczywistości wirtualnej.

Czy wiemy jak się przed nimi zabezpieczyć? Odpowiedzią na to pytanie są wyniki badania dotyczącego cyberbezpieczeństwa, które przeprowadzono na zlecenie Fundacji Kronenberga Citi Handlowy.

[1] *Jak Polacy korzystają z telefonu i internetu w czasie pandemii,* raport KDR, lipiec 2020 https://krd.pl/Centrum-prasowe/Raporty/2020/Jak-Polacy-korzystaja-z-telefonu-i-Internetu-w-czasie-pandemii

[2] *Nowa rzeczywistość: konsument w dobie COVID-19,* raport KPMG, Wrzesień 2020 https://assets.kpmg/content/dam/kpmg/pl/pdf/2020/09/pl-Raport-KPMG-Nowa-rzeczywistosc-konsument-w-dobie-COVID-19.pdf

54,3%
spędza więcej czasu online

71%
rezygnuje z wizyt w sklepie stacjonarnym
(produkty inne niż spożywcze)

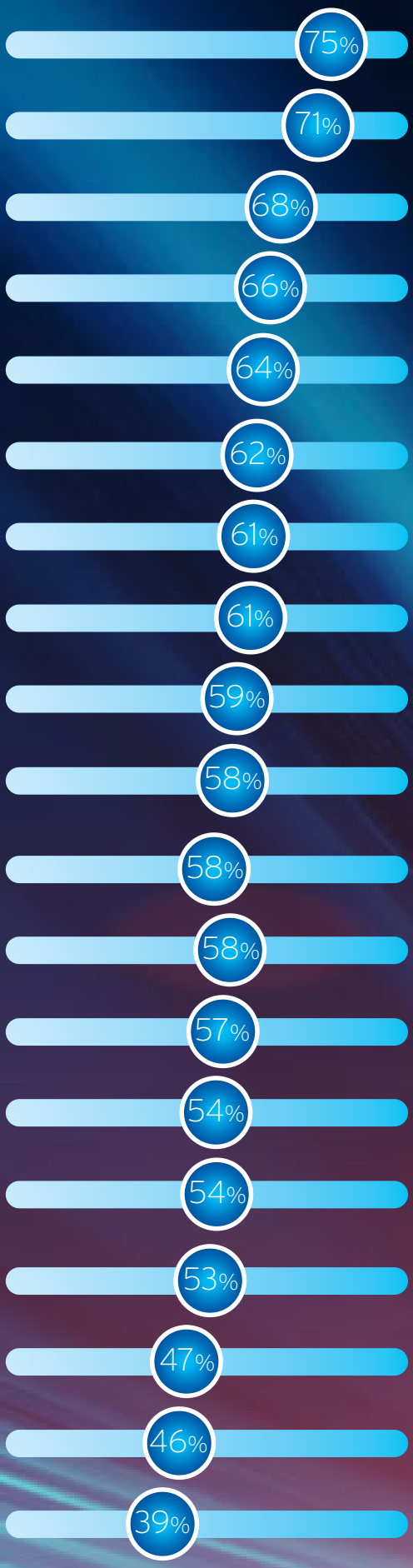
Mamy świadomość, że jako użytkownicy internetu jesteśmy narażeni na różne zagrożenia. Prawie wszyscy zetknęliśmy się z tym tematem. Tylko 6% Polaków nigdy nie słyszała o niebezpieczeństwach w sieci. Najczęściej dowiadujemy się o nich z mediów – 68% badanych właśnie tam słyszała o cyberzagrożeniach. Co ważne, **wielu z nas bezpośrednio spotkało się z zagrożeniami w internecie – co druga osoba przyznaje, że ona sama lub ktoś z jej z otoczenia doświadczyli niebezpiecznych sytuacji w sieci.** Więcej osobistych doświadczeń z cyberzagrożeniami mają najmłodsi internauci (15–17 lat), a najmniej osoby po 45. roku życia.

68%
badanych dowiaduje się o cyberzagrożeniach z mediów

Przeciętny Polak zdaje sobie sprawę z 11 zagrożeń istniejących w sieci. Najbardziej świadomi jesteśmy przestępstw polegających na wyłudzaniu pieniędzy poprzez płatne SMS-y i ogłaszane w sieci fałszywe konkursy czy zbiórki – ponad 70% z nas zna taką formę oszustwa. Zdecydowana większość zdaje sobie także sprawę z istnienia wirusów i możliwości ściągnięcia ich na swój komputer lub telefon poprzez kliknięcie w fałszywy link (68%) czy zainstalowanie zainfekowanego oprogramowania (66%). Wiemy również o takich metodach działania złodziei jak: kradzież danych osobowych w celu wzięcia na nie kredytu/pożyczki (64%), włamanie na konto bankowe (62%) czy podszywanie się pod kogoś bliskiego, żeby wyłudzić pieniądze (61%).

Gorzej jest z naszą świadomością oszustw polegających na blokowaniu sprzętu i próbach wyłudzenia pieniędzy na jego odblokowanie, możliwości dokonywania operacji finansowych za pomocą skradzionego telefonu/komputera czy przejęcia środków podczas dokonywania płatności w sieci. O takich zagrożeniach słyszała mniej niż połowa internautów.

ŚWIADOMOŚĆ RÓŻNYCH TYPÓW ZAGROŻEŃ



płatne SMS-y

fałszywe konkursy i zbiórki pieniędzy

kliknięcie w link z maila, który zainfekuje konputer/telefon

zawirusowanie komputera/instalacja złośliwego oprogramowania

wyłudzenia kredytów przy użyciu danych osobowych

włamanie się na konto, kradzież pieniędzy z konta bankowego

podszywanie się pod kogoś/bliską osobę w celu wyłudzenia przelewu pieniędzy

oszustwa sklepów internetowych, nieuczciwych dostawców

nakładka na bankomat zainstalowana przez złodziei – kradzież PIN-u

kliknięcie w link z SMS-a, który zainfekuje telefon

wyłudzenia danych osobowych (np. w odp. na fałszywy mail, SMS)

wypłaty pieniędzy, płatności robione z ukradzionej karty

podszywanie się pod instytucję/firmę w celu wyłudzenia pieniędzy i/lub skłonienia do otwarcia zainfekowanego załącznika

kliknięcie w link z wiadomości prywatnej/w poście w social mediach

kradzież prywatnych zdjęć, filmów lub skanów dokumentów

szkalowanie, szantażowanie i kompromitowanie w mediach społecznościowych

włamanie na konto/pobranie środków podczas transakcji w internecie

kradzież, wyłudzenia, zakupy w ramach bankowości online przy wykorzystaniu ukradzionego/zagubionego telefonu

zablokowanie sprzętu (komp./tel.) i żądanie okupu za ich włączenie

Cyberbezpieczeństwo użytkowników banków, raport przygotowany przez IQS na zlecenie Fundacji Kronenberga Citi Handlowy, marzec 2020. Próba, N=1111 w wieku 15-55 lat.

NAJBARDZIEJ OBAWIAMY SIĘ ZAGROŻEŃ ZWIĄZANYCH ZE STRATĄ PIENIĘDZY, A PONADTO:

65% zawirusowania sprzętu

62% nieuczciwych sprzedawców w internecie

62% włamań na konto

60% kradzieży danych osobowych

Z przeprowadzanego badania wynika, że polscy internauci najbardziej boją się przestępstw związanych ze stratą finansową, dokonanych bez świadomości osoby okradanej. Większość deklaruje, że obawia się zawirusowania sprzętu (65%), nieuczciwych sprzedawców w interencie (62%), włamań na konto (62%) czy wzięcia kredytu za pomocą skradzionych danych osobowych (60%). Z kolei przestępstwa, do których dochodzi przy aktywnym udziale osoby poszkodowanej, jak odsyłanie płatnych SMS-ów, wpłacanie pieniędzy na fałszywe zbiórki czy klikanie w linki z niebezpiecznych źródeł – mimo że są powszechnie znane – budzą mniejsze obawy. Boi się ich mniej niż połowa polskich internautów.

> *Spodziewamy się konkretnych ataków na nasze konto bankowe, sprzęt czy ze strony fałszywych sklepów internetowych – bo o takich atakach słyszymy najczęściej w mediach. Natomiast to, co budzi nasze mniejsze obawy, spowodowane jest raczej brakiem naszej świadomości dotyczącej takich rodzajów lub metod ataków. Brak świadomości to mniejsza czujność.*

Strony wyłudzające dane osobowe oraz dane uwierzytelniające są obecnie zjawiskiem masowym, z którym stykają się różne grupy użytkowników internetu w Polsce. Linki do nich przesyłane są różnymi kanałami: przez SMS-y, maile lub w mediach społecznościowych.

Przykład: cyberprzestępcy połączyli dwa oszustwa w jedno i próbują straszyć polskich użytkowników. Wysyłają im wiadomości z informacją o usłudze SMS Premium, która dziennie będzie obciążać nasz rachunek kwotą ponad 30 złotych. W SMS-ie oferują możliwość zrezygnowania z kosztownej subskrypcji i zalecają kliknięcie w specjalny link, który przenosi do strony z anulowaniem zamówienia. Oczywiście, pod żadnym pozorem nie należy tego robić! Pytanie: jak wiele osób jest tego świadomych?

W linku do rezygnacji będzie podstawiona fałszywa strona popularnej formy płatności, np. Dotpay. Tam cyberprzestępcy będą próbowali przejąć dane logowania do banku. Pod informacjami o anulowaniu subskrypcji w rzeczywistości kryje się potwierdzenie przelewu – w ten sposób nie tylko wysyłamy pieniądze hakerom i zgadzamy się na obciążenie rachunku, lecz także dajemy im pełny dostęp do danych logowania na nasze konto w banku.”

Andrzej Grabowski,
ekspert ds. COB i kontroli bezpieczeństwa informacji

MOCNE STRONY ZWIĄZANE Z OCHRONĄ PRZED CYBERZAGROŻENIAMI

Twierdzimy, że przywiązujemy dużą wagę do kwestii bezpieczeństwa w internecie – prawie 60% badanych deklaruje, że jest ono dla nich ważne.

Jesteśmy świadomi istnienia wirusów, które mogą nam zainfekować sprzęt i wykraść nasze dane. Dlatego aktualizujemy programy antywirusowe i staramy się unikać otwierania nieznanych załączników oraz klikania w podejrzane linki.

Do aplikacji podchodzimy przezornie i z ostrożnością, choć nie zawsze się to udaje. Sprawdzamy, do jakich danych wymaga dostępu nowa aplikacja, którą instalujemy. 42% Polaków robi to zawsze, a co trzeci – czasami.

Najbardziej chronimy numery naszych kart kredytowych – 69% Polaków nigdy ich nie udostępnia.

Staramy się podchodzić rozsądnie do dzielenia się naszymi danymi online. Większość z nas nie udostępnia informacji z dowodu tożsamości oraz numeru PESEL. Jeśli już przekazujemy komuś informacje o sobie, to zwykle podajemy wybranym instytucjom to głównie dane kontaktowe lub adres zamieszkania, ale także informacje o naszych poglądach i zainteresowaniach.

Wraz z pojawieniem się internetu, a przede wszystkim mediów społecznościowych, zatarły się w naszej świadomości granice tego, co kiedyś określane było jako osobiste, by nie powiedzieć: intymne. Jeszcze dwadzieścia lat temu naszym światopoglądem, politycznymi preferencjami czy wyznawaną religią dzieliliśmy się z najbliższymi – rodziną, przyjaciółmi, wspólnotą. Dzisiaj chętnie wrzucamy na nasze Insta Stories, tablice czy TikToki to, co aktualnie myślimy, w czym bierzemy udział, co przeczytaliśmy, i opatrujemy komentarzem. Przy czym ten ostatni co jest znakiem czasu, też przybiera różne formy: od wypowiedzi słownej po emotki – smutne, roześmiane, złe itd. Trudno wskazać, że jest to zjawisko jednoznacznie negatywne, szczególnie w dobie pandemii, kiedy kontakt jest tak bardzo ograniczony. Możliwość dzielenia się swoimi przemyśleniami i komentowania daje poczucie wspólnoty i pozwala na komunikację z bliskimi, choćby w tak okrojonej wersji. Niemniej warto pamiętać, że jeśli nie zabezpieczymy swoich profili we właściwy sposób, dostęp do informacji o nas będzie miało szerokie gremium. Nie wiemy lub nie pamiętamy, że pracodawcy coraz częściej weryfikują informacje na nasz temat w publicznie dostępnych zasobach internetowych, w tym również w mediach społecznościowych! Nawet jeśli nie publikujemy danych, ale często dajemy „polubienia", „serduszka", opinie, to na tej podstawie dział kadr może zbudować sobie nasz wizerunek. Już teraz część firm zastrzega podczas rekrutacji, że odezwie się wyłącznie do kandydatów przystających do „profilu firmy" – to oznacza, że potencjalnym pracownik zostanie sprawdzony pod kątem informacji możliwych do znalezienia na jego temat w sieci. Jeśli publikujemy skrajne poglądy nasze szanse na zatrudnienie w międzynarodowej korporacji, gdzie pracuje się w zróżnicowanym środowisku, maleją do zera; zdjęcie z papierosem wykluczy nas jeśli firma profiluje się jako ekologiczna, alkohol w ręku – nawet na rodzinnym przyjęciu – będzie dyskredytujący, jeśli szukamy zatrudnienia w zawodach zaufania publicznego. Dlatego tak ważne jest rozsądne gospodarowanie informacjami o nas samych. Pamiętajmy, że nie tylko to, jakie reklamy do nas trafią, ale i to czy znajdziemy pracę, zaczyna zależeć od naszego wizerunku w przestrzeni wirtualnej. Zadbajmy o to, żeby informacje były podzielone i trafiały do właściwych grup odbiorców. Oddzielmy to co publiczne, od tego, co prywatne – na szczęście zarówno tak internet, jak i media społecznościowe dają taką możliwość. Wymaga to jednak rozsądku i przemyślenia strategii wizerunkowej.

Berenika Anders-Mosakowska,
prawniczka, ekspertka strategii audytu komunikacji cyfrowej oraz ochrony wizerunku online

SŁABE STRONY ZWIĄZANE Z OCHRONĄ PRZED CYBERZAGROŻENIAMI

Cyberbezpieczeństwo użytkowników banków, raport przygotowany przez IQS na zlecenie Fundacji Kronenberga Citi Handlowy, marzec 2020. Próba, N=1111 wieku 15-55 lat.

Zdecydownie się zgadzam

Zdecydownie się zgadzam + raczej się zgadzam

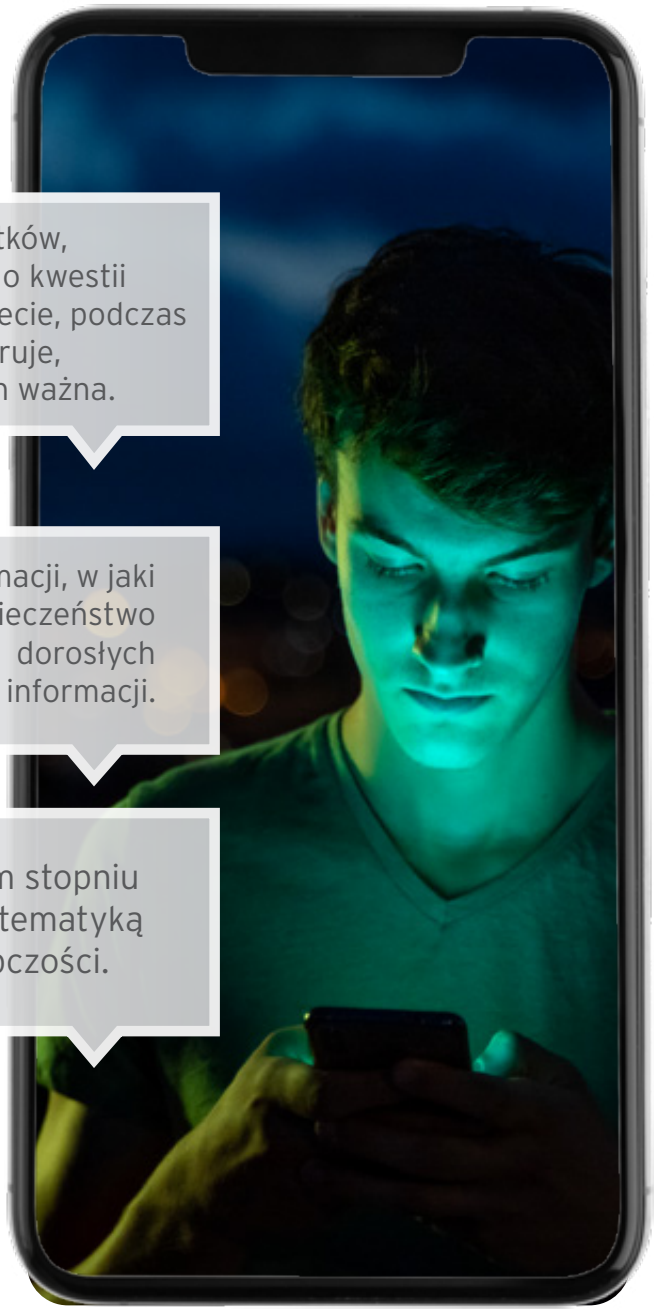
Tylko co trzeci z nas uważa, że ma wiedzę na temat cyberzagrożeń i umie się przed nimi chronić. Ponadto mniej niż połowa użytkowników internetu stara się poszerzać swoją wiedzę o tym, jak zachowywać się bezpiecznie w sieci.

To, w jaki sposób korzystamy z internetu, zależy od naszego wieku. Młodzież jest bardziej aktywna w sieci i korzysta z niej w różnorodny sposób. Portale społecznościowe są naturalnym środowiskiem nastolatków.

75% nastolatków ma sześć lub więcej kont na różnych portalach – średnio każdy ma siedem kont. Starsi także nie stronią od portali, ale korzystają z nich mniej intensywnie.

22% osób w wieku 40–49 lat ma sześć lub więcej kont, a średnio te osoby mają cztery konta. Więcej młodzieży korzysta też z subskrypcji dających dostęp do płatnych treści, usług, produktów – robi tak 45% osób w wieku 15–19 lat i 21% osób w wieku 40–49 lat.

Wiedza oraz świadomość cyberzagożeń także zależą od wieku. Mimo że młodzież bardziej intensywnie korzysta z internetu, przejawia mniejsze zainteresowanie tematem cyberzagrożeń i mniej wie na ich temat.



48%
osób w wieku 15-19 lat

Mniej niż połowa nastolatków, przywiązuje dużą wagę do kwestii bezpieczeństwa w internecie, podczas gdy 61% dorosłych deklaruje, że ta kwestia jest dla nich ważna.

Tylko jedna trzecia nastolatków szuka informacji, w jaki sposób można i należy dbać o swoje bezpieczeństwo w internecie, podczas gdy prawie połowa dorosłych (48% osób w wieku 40–55 lat) szuka takich informacji.

53%
nastolatków

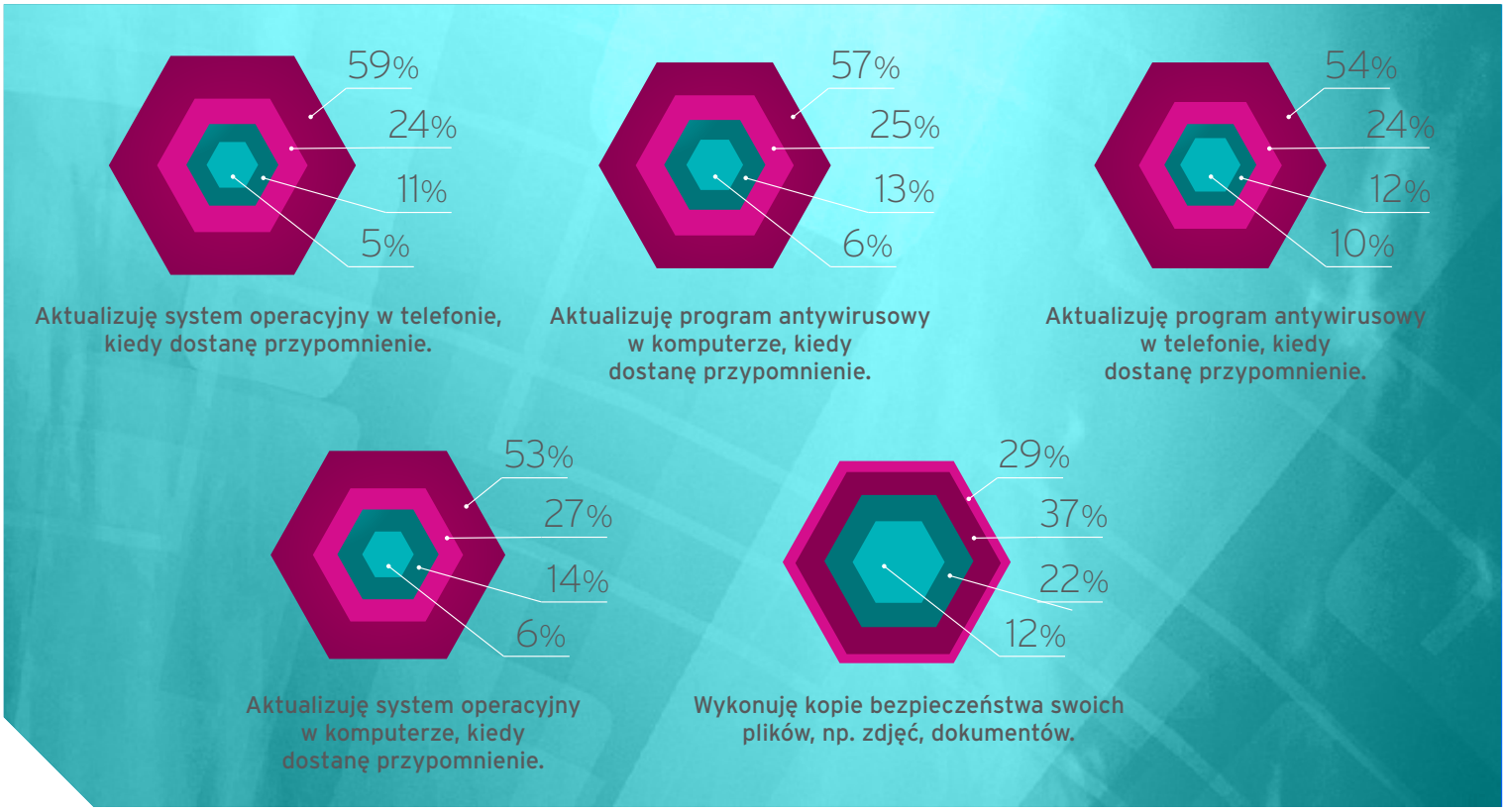
w największym stopniu interesuje się tematyką cyberprzestępczości.

Młodzi ludzie mają też większe poczucie, że znają się na zabezpieczeniach w internecie – tylko 16% nastolatków twierdzi, że słabo zna się na zabezpieczeniach i nie wie, jak się chronić. Dwa razy większy odsetek dorosłych deklaruje słabą znajomość zabezpieczeń internetowych (32% osób w wieku 30–39 lat oraz 34% osób w wieku 40–55 lat).

Nasza ignorancja w kwestii cyberzagrożeń sprawia, że nie zawsze udaje nam się zachować ostrożność i czujność, przez co narażamy się na niebezpieczeństwa czyhające na nas w sieci. Często różne czynności wykonujemy „automatycznie", nie zastanawiając się nad sensem naszych poczynań. Dzieje się tak w różnych sferach naszej aktywności

AKTUALIZACJA SYSTEMÓW

Powszechnie aktualizujemy systemy antywirusowe i operacyjne w telefonach lub komputerach. Do tematu aktualizacji systemów antywirusowych różnie podchodzą dorośli i młodzież. Mniej niż połowa młodzieży aktualizuje systemy operacyjne i antywirusowe, kiedy dostaje przypomnienie, a najrzadziej robią to nastolatkowie – 40% z nich (15–19 lat) zawsze aktualizuje program antywirusowy w telefonie, a 43% – w komputerze. Starsi przywiązują do tego większą wagę – 64% osób w wieku 30–39 lat oraz 62% osób w wieku 40–55 lat zawsze aktualizuje program antywirusowy w komputerze, kiedy dostaje przypomnienie. Dorośli bardziej pilnują aktualizowania systemu. Zwykle jednak decydują się na to, kiedy dostają przypomnienie, i często wykonują operację w nocy, żeby nie przeszkadzała im w korzystaniu z urządzenia.

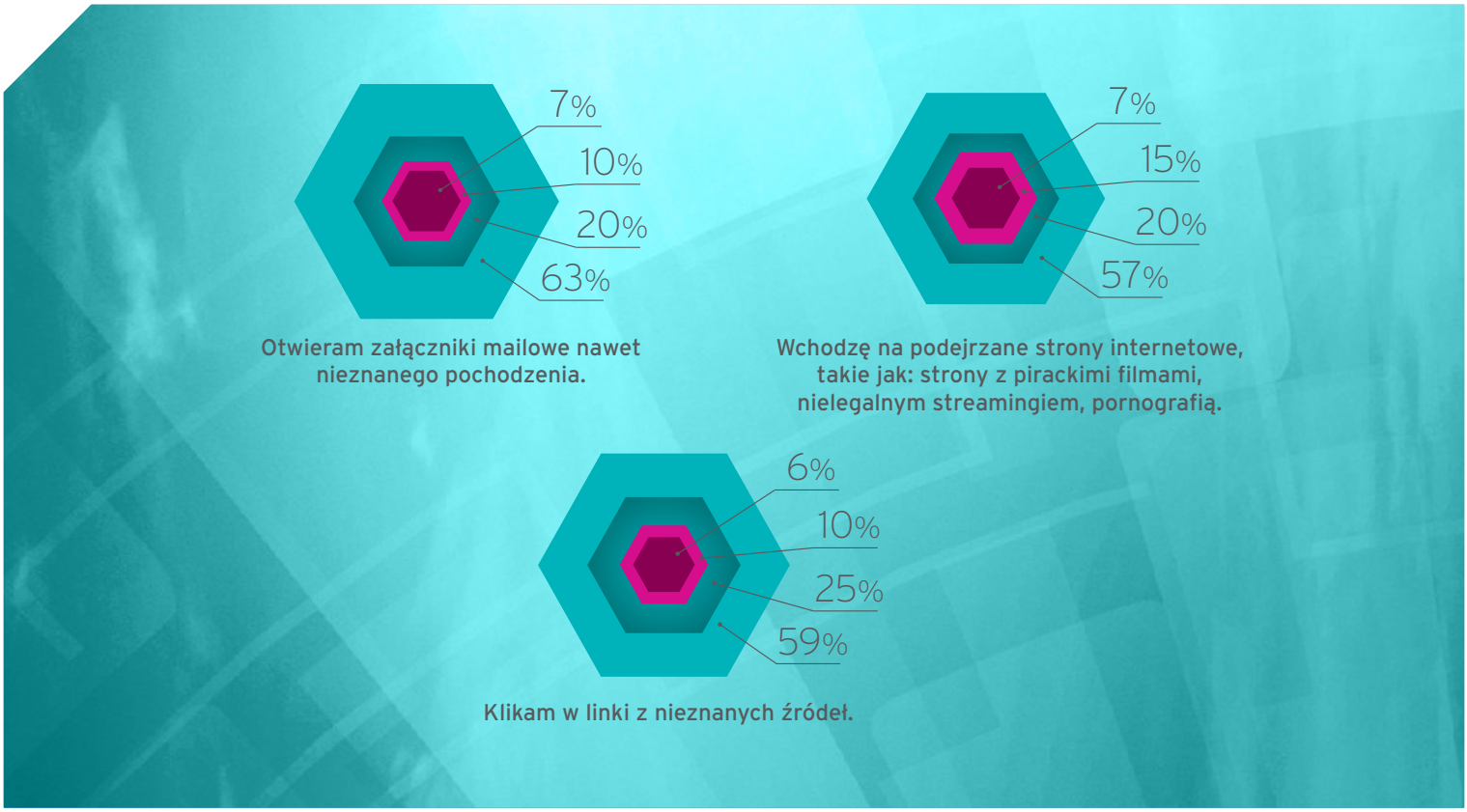


Cyberbezpieczeństwo użytkowników banków, raport przygotowany przez IQS na zlecenie Fundacji Kronenberga Citi Handlowy, marzec 2020. Próba, N=1111 w wieku 15–55 lat.

NIEZNANE MAILE I ZAŁĄCZNIKI

Pomimo świadomości istnienia cyberzagrożeń nadal wielu z nas przez ciekawość lub nieuwagę ulega niebezpiecznym pokusom i w dodatku nie budzi to w nas większych obaw. 43% Polaków zdarza się odwiedzać podejrzane portale: strony z pirackimi filmami, nielegalnym streamingiem, pornografią. 41% zdarza się klikać w linki z nieznanych źródeł, a 37% – otwierać załączniki mailowe nieznanego pochodzenia.

Częściej ryzykownym zachowaniom ulega młodzież – prawie połowie nastolatków zdarza się otwierać załączniki mailowe nieznanego pochodzenia (54% osób w wieku 15–19 lat nigdy tego nie robi). Im jesteśmy starsi, tym bardziej potrafimy oprzeć się ciekawości, zachować ostrożność i nie otwierać nieznanych wiadomości.

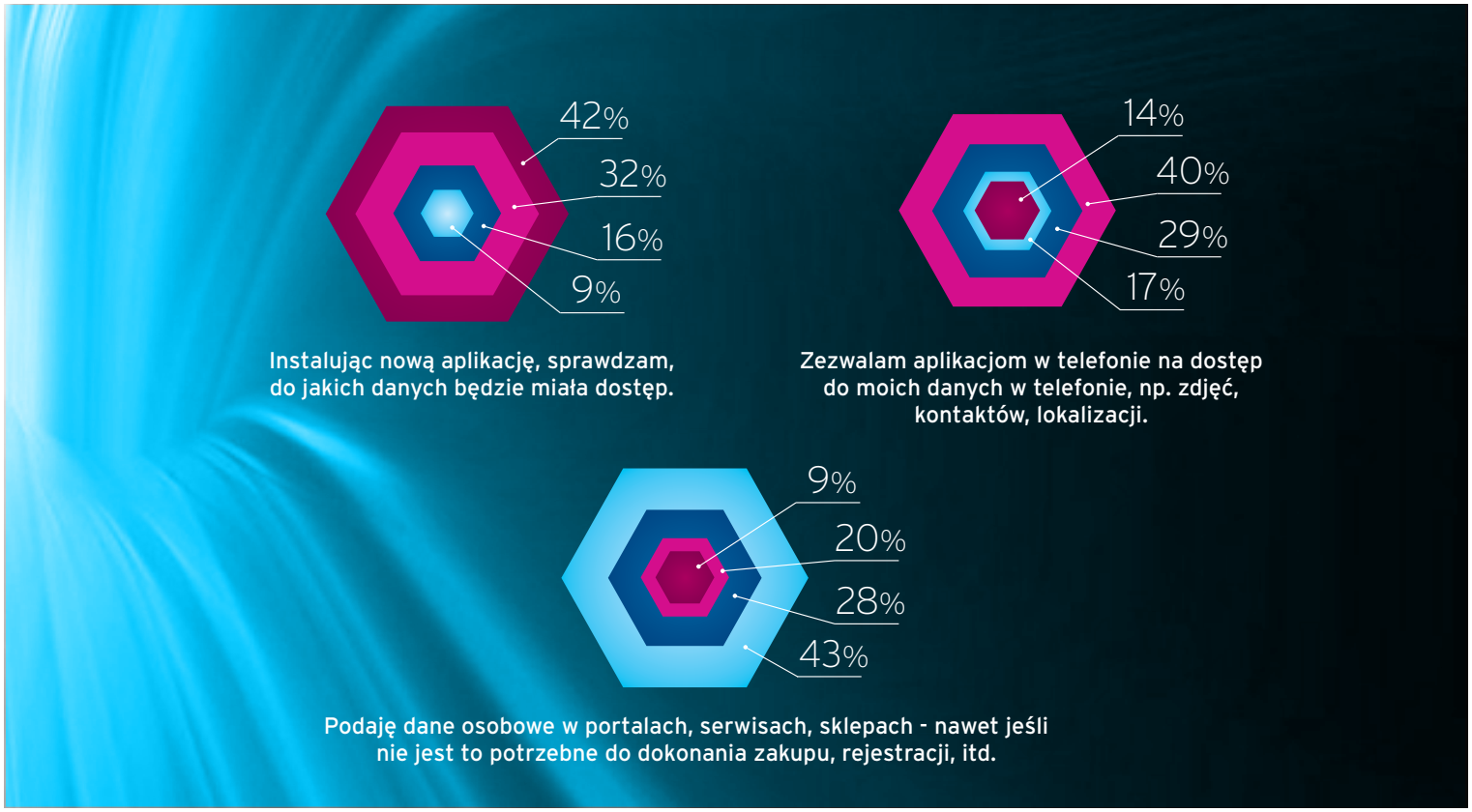


Cyberbezpieczeństwo użytkowników banków, raport przygotowany przez IQS na zlecenie Fundacji Kronenberga Citi Handlowy, marzec 2020, Próba, N=1111 w wieku 15–55 lat.

DZIAŁANIE URZĄDZEŃ MOBILNYCH I APLIKACJI

Dwie trzecie z nas unika podawania swoich danych osobowych w internecie. Jednocześnie spora część Polaków korzysta z serwisów i aplikacji, w których trzeba udostępniać swoje dane – robi tak 38% osób. Zezwalamy aplikacjom w telefonie na dostęp do naszych danych, np. zdjęć, kontaktów, lokalizacji – tylko 17% Polaków twierdzi, że nigdy tego nie robi. Chętnie zgadzamy się też na wszystkie wymagania aplikacji internetowych i podajemy im informacje o sobie, nawet jeśli nie są one konieczne dla ich działania – zdarza się to robić 57% Polaków.

Jeśli chodzi o udostępnianie danych, młodzież chętniej niż dorośli podaje informacje osobowe w portalach, serwisach i sklepach, nawet jeśli nie są one kluczowe dla dokonania zakupu – tylko 34% nastolatków nigdy tego nie robi. 49% osób w wieku 40–55 lat nigdy nie podaje takich informacji.



Cyberbezpieczeństwo użytkowników banków, raport przygotowany przez IQS na zlecenie Fundacji Kronenberga Citi Handlowy, marzec 2020, Próba, N=1111 w wieku 15–55 lat.

Złośliwe oprogramowanie na urządzenia mobilne często wygląda jak normalna aplikacja. Dzięki niemu osoby trzecie mogą śledzić aktywność użytkownika i uzyskiwać dostęp do cennych danych, np. numerów kart kredytowych czy danych bankowych.

Aplikacja może np. uzyskiwać dostęp do książki adresowej. Dane te są bardzo atrakcyjnym łupem dla spammerów i oszustów. Uprawnienie to umożliwia także dostęp do wszystkich kont, z których korzystasz na danym urządzeniu, np. w serwisach Google, Facebook, Instagram itp.

Andrzej Grabowski,
ekspert ds. COB i kontroli bezpieczeństwa informacji

UMIESZCZANIE SWOJEGO WIZERUNKU W INTERNECIE

Czterech na pięciu Polaków dzieli się swoimi przekonaniami w sieci. Często takie informacje wykorzystywane są do tworzenia wszechobecnych sprofilowanych kampanii marketingowych i reklam. Dwie trzecie z nas udostępnia też w internecie swój wizerunek oraz informacje o swojej lokalizacji.

„Niezadowolonym z informacji, jakie można znaleźć na swój temat w internecie, przychodzi w sukurs prawo do bycia zapomnianym. Zostało ono sformułowane w wyroku Trybunału Sprawiedliwości z dnia 13 maja 2014 r. (C-131/12) w kontekście sporu, który zaistniał pomiędzy Google Spain SL oraz Google Inc. a Agencia Española de Protección de Datos (hiszpańską agencją ochrony danych, odpowiednikiem polskiego UODO) i Mariem Costeja Gonzálezem. Wpisując bowiem imię i nazwisko Gonzáleza w wyszukiwarce Google, otrzymywało się na jednej z czołowych pozycji link do ogłoszenia w gazecie „La Vanguardia", informującego o komorniczej licytacji jego nieruchomości. Pan González, który dawno spłacił swoje długi (ogłoszenie pochodziło z 1998 r.), a w internecie wciąż miał wizerunek niepoprawnego dłużnika, zwrócił się ze skargą do agencji, żądając, aby jego dane osobowe nie były ujawniane w wynikach wyszukiwania i nie były powiązane z linkami do ogłoszenia w gazecie La Vanguardia. Sprawa ostatecznie trafiła do Trybunałem Sprawiedliwości Unii Europejskiej, który orzekł, że skoro Google przetwarza dane osobowe, jako administrator ma obowiązek uczynienia zadość żądaniu pana Gonzáleza.

Konsekwencją wyroku było wprowadzenie „prawa do bycia zapomnianym" do przepisów Rozporządzenia o ochronie danych osobowych (RODO). Art. 17 RODO określa kiedy prawo to może znaleźć zastosowanie. Wymienia się tu cofnięcie zgody na przetwarzanie danych w sytuacji, gdy była ona podstawą ich przetwarzania oraz sprzeciw wobec przetwarzania danych osobowych na potrzeby i w zakresie marketingu bezpośredniego (w tym profilowania). W sposób szczególny traktuje się dane osobowe, które zostały zebrane w związku z oferowaniem usług internetowych, np. usług portalu społecznościowego, osobom poniżej 16. roku życia.

Żądanie usunięcia danych nie zostanie spełnione, jeśli przetwarzanie danych jest niezbędne do korzystania z prawa do wolności wypowiedzi i informacji, wywiązania się z prawnego obowiązku, z uwagi na interes publiczny w dziedzinie zdrowia publicznego, jak również gdy jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych, historycznych lub statystycznych albo do ustalenia, dochodzenia bądź obrony roszczeń.

Zgodnie ze statystykami Google, niemal połowa żądań o usunięcie danych osobowych jest rozpatrywana pozytywnie."

dr Agnieszka Besiekierska
Prawniczka, jedna z TOP-20 Cybersecurity Women in Poland.

Umieszczanie zdjęć w sieci to standardowa czynność, jednak źle wykonana może stać się dla nas poważny problem. Przede wszystkim sami użytkownicy w serwisów społecznościowych nie chronią swojej prywatności, wrzucając do sieci wiele zdjęć, z którymi nie wiadomo co później się dzieje. Jak wiemy, w internecie nic nie ginie, ale często się zdarza, że nasze zdjęcia za pośrednictwem „wianuszka" znajomych i nieznajomych mogą wypłynąć na innych serwisach.

W mediach społecznościowych nie jesteśmy jedynie biernymi widzami. Relacjonując w nich wydarzenia z naszego życia i umieszczając zdjęcia, sami udostępniamy informacje, które mogą stać się źródłem późniejszych problemów. Często zdjęcia są kradzione z profili w mediach społecznościowych, a w konsekwencji może dojść do naruszenia prawa w kwesti wykorzystania tych zdjęć bez naszej zgody i wiedzy.

1 Twoje zdjęcie nie zniknie wraz z usunięciem przez ciebie profilu w mediach serwisie społecznościowym. Każde zdjęcie umieszczone w internecie podlega archiwizacji, a potem jest dostępne poprzez wyszukiwarkę. Innymi słowy – zaczyna żyć własnym życiem wraz z wrzuceniem go przez ciebie do sieci. Co więcej, niektóre strony internetowe zastrzegają sobie prawo do nieodpłatnego wykorzystywania zdjęć zamieszczonych na prywatnych profilach użytkowników.

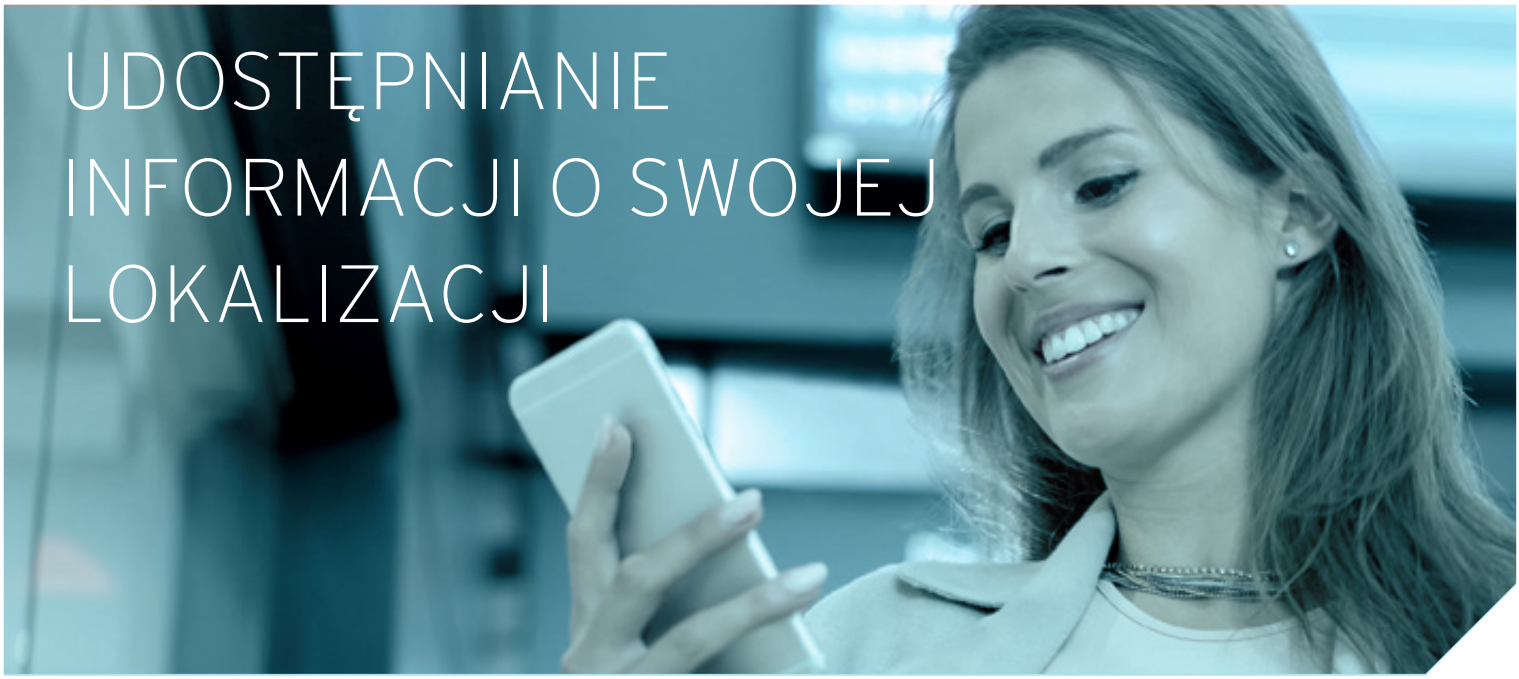
2 Zanim opublikujesz np. zdjęcie swojego dziecka, zadaj sobie pytanie: czy moje dziecko chciałoby kiedyś zobaczyć to zdjęcie w sieci? Kiedyś ono dorośnie i zobaczy, w jaki sposób zostało pokazane w sieci przez swoich rodziców.

Prawo do prywatności przysługuje wszystkim – również dzieciom. Z pozoru niewinna i zabawna fotka na nocniku może w przyszłości stać się przyczyną szykanowania twojego dziecka przez rówieśników.

3 Twoje zdjęcie w sieci może zostać wykorzystane przez inne osoby bez twojej wiedzy. Ludzie tworzą strony internetowe, grupy w mediach społecznościowych czy kompilacje zdjęć na YouTubie, gdzie wykorzystują różne zdjęcia z internetu.

4 *Last – but not least* – publikowane przez ciebie zdjęcia mogą również zobaczyć pedofile. Latem wrzucamy do sieci mnóstwo zdjęć z wakacji. Część z nich to ujęcia nagich lub półnagich dzieci, bez bielizny czy pieluchy. Zanim zdecydujemy się upublicznić takie fotki, zastanówmy się, czy chcielibyśmy, aby trafiły do ludzi, który potraktują je jak pedofilską pornografię.

UWAGA: TYLKO ŚWIADOMOŚĆ ORAZ ZDROWY ROZSĄDEK MOGĄ NAS URATOWAĆ!



UDOSTĘPNIANIE INFORMACJI O SWOJEJ LOKALIZACJI

Wrzucasz na Facebooka informację, że właśnie jesz pyszny posiłek w restauracji w centrum Warszawy?

Udostępniasz lokalizację na swoim koncie na Instagramie?

A może uwielbiasz robić zdjęcia i starasz się, aby każde z nich zawierało informację o miejscu, w którym zostało zrobione?

UJAWNIASZ W TEN SPOSÓB ADRESY, KTÓRE INNE OSOBY MOGĄ WYKORZYSTAĆ PRZECIWKO TOBIE.

Kiedy meldujesz się, zamieszczasz zdjęcia lub robisz coś, co wiąże się z podaniem współrzędnych GPS, możesz tym samym ujawnić, gdzie dokładnie przebywasz. Jeżeli robisz to z własnego domu lub mieszkania swoich znajomych, publicznie ujawniasz ich lokalizację, ryzykując, że ktoś z was padnie ofiarą włamywacza.

Jeśli wrzucisz na Facebooka informację o tym, że właśnie rozpoczynasz dwutygodniowe wakacje na Krecie, złodziej będzie miał sporo czasu, aby przygotować włamanie.

Jeżeli zameldowałeś się w restauracji, nie możesz być w tym samym czasie w swoim domu. Dowiedzą się o tym twoi przyjaciele, a jeżeli ogłosisz tę informację na Twitterze – także potencjalni złodzieje polujący na swoje ofiary na portalach społecznościowych, którzy – jeżeli wiedzą lub potrafią określić, gdzie mieszkasz – mogą włamać się do twojego domu.

Zabezpiecz sprzęt, którego używasz – jeśli robisz smartfonem zdjęcie, wyłącz zapisywanie lokalizacji w metadanych zdjęcia. W ten sposób uchronisz się przed podaniem informacji, w jakim miejscu zdjęcie zostało wykonane.

Typową sztuczką oszustów jest udostępnienie strony głównej, zawierającej np. zdjęcia lub filmy dostępne w krótkim, bezpłatnym okresie próbnym.

Po zarejestrowaniu użytkownik odkrywa, że jednak nie może uzyskać dostępu do obiecanej zawartości. Nie zapłacił, więc może mu się wydawać, że nic złego się nie wydarzyło, i prawdopodobnie całą sytuację zignoruje. Niestety, kilka dni później odbierze fakturę, na kwotę kilkuset euro za roczną subskrypcję. Będzie ona zawierać informację, że bezpłatny okres próbny został automatycznie zmieniony na roczną subskrypcję. Oprócz sprzedaży fałszywych subskrypcji witryny te czerpią zyski z wyłudzania danych, np. sprzedają informacje wprowadzone przez użytkowników podczas rejestracji.

Po rejestracji niektóre fałszywe witryny rozsyłają nawet, za pośrednictwem poczty elektronicznej lub SMS-ów, wiadomości prywatne z informacją o tym, że ze względów bezpieczeństwa wymagana jest większa ilość danych osobowych. Wszystkie dane są gromadzone w celu późniejszej sprzedaży, często zostają użyte na potrzeby innych nielegalnych przedsięwzięć.

Dla dorosłych najpoważniejsze zagrożenia to takie, które mają bezpośrednie przełożenie na poziom życia i wiążą się z długotrwałą chorobą, długami finansowymi czy brakiem środków do życia. Pandemia jeszcze bardziej wzmocniła te obawy i zagrożeniami. Dorośli nie uważają cyberprzestępczości za poważne zagrożenie dla funkcjonowania. Szczególnie w czasach pandemii wydaje się ona mało rzeczywista, nienamacalna.

Dorośli radzą sobie z codziennymi zagrożeniami, bazując na sprawdzonych metodach, uczeniu się na błędach albo cedują odpowiedzialność na innych (np. ubezpieczenia i produkty zapewniające poczucie bezpieczeństwa). Jednak żaden z tych sposobów nie sprawdza się przy cyberzagrożeniach, bowiem ciągle pojawiają się nowe i wciąż musimy się uczyć im przeciwdziałać, do czego nie jesteśmy przyzwyczajeni. Podchodzimy do tego z oporem i niechęcią albo stwierdzamy, że nie mamy czasu zajmować się tymi sprawami teraz, kiedy mierzymy się ze skutkami pandemii. Dlatego zwykle na informacje o zagrożeniach online reagujemy pasywnością lub fatalizmem, przekonani, że nie da się im zapobiec.

Najsłabszym ogniwem cyberbezpieczeństwa jest człowiek. Często przestępcy nawet nie próbują się mierzyć z wyszukanymi zabezpieczeniami technicznymi, tylko kierują atak na użytkownika, wykorzystując inżynierię społeczną (social engineering). Perfidnie uderzeni w czuły punkt ludzkich potrzeb emocjonalnych: potrzeb ważności i akceptacji, potrzeby komfortu w trudnych czasach czy empatii i uczynności, tracimy pieniądze i narażamy się na dodatkowy stres. Podczas pierwszego lockdownu pojawiły się aplikacje z mapami, przedstawiające rozprzestrzeniane się epidemii, które po ściągnięciu blokowały dostęp do urządzenia i żądały okupu. Na popularnym portalu prowadzącym zbiórki charytatywne pojawiła się ciesząca się dużym zainteresowaniem zbiórka na cel zaopatrzenia w środki ochrony pracowników medycznych. Jak się okazało pieniądze nigdy nie trafiły do zainteresowanych.

Ofiarą padają nie tylko zwykli obywatele, ale również prezesi największych firm technologicznych (inżynieria społeczna kierowana do kadry zarządzającej to tzw. whaling, czyli łowienie wielorybów) i największe światowe koncerny. Dwa lata temu szerokim echem w mediach odbił się tzw. atak na pizzerię, w ramach którego pracownicy, skuszeni promocyjnymi cenami pizzy, a następnie gratisowym prezentem w postaci mrugających lampek na USB, zawiesili działanie całego systemu IT w firmie. Chociaż atak był pozorowany, to emocje i zachowanie nieświadomych pracowników – w 100% autentyczne.

Dlatego niezwykle istotna jest świadomość zagrożeń, obejmująca wszystkich i wszystkie szczeble organizacji. Budowaniu świadomości w organizacji sprzyjają odpowiednie ramy prawno-organizacyjne dotyczące cyberbezpieczeństwa. Obejmują one politykę i regulaminy bezpieczeństwa określające kategorie informacji poufnych i zakresy odpowiedzialności uwzględniające przepisy dotyczące bezpieczeństwa informacji oraz systemów IT wzorowane na sprawdzonych międzynarodowych standardach oraz spersonalizowane umowy o poufności z pracownikami i współpracownikami. Ważny jest zinstytucjonalizowany program szkoleń pracowniczych o ciągłym charakterze, aktualizowany w zależności od potrzeb i rozwoju wypadków.

dr Agnieszka Besiekierska

MŁODZIEŻ A ZAGROŻENIA ONLINE

Dla młodzieży cyberzagrożenia związane z finansami to problem, z którym zetkną się dopiero w przyszłości. Wśród nastolatków panuje przekonanie:

> *„Wiem, że to może mnie dotyczyć w przyszłości, ale teraz nawet nie mam jeszcze własnych pieniędzy."*

Młodzi uważają, że mają obecnie zbyt mało pieniędzy, aby być atrakcyjnym celem ataku ze strony cyber złodziei.

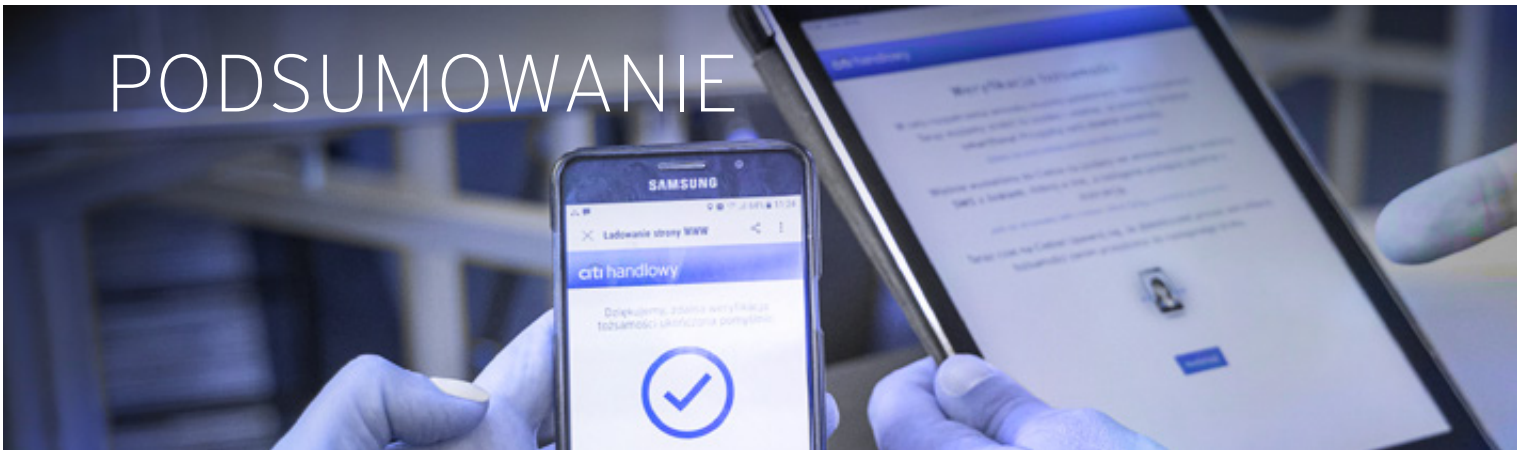
Nie znaczy to, że nie spotykają się z „ciemną" stroną internetu. Deklarują doświadczenia z phishingiem, hejtem, a nawet z propozycjami sponsoringu seksualnego. Podczas pandemii młodzi ludzie są jeszcze bardziej narażeni na te niebezpieczeństwa, ponieważ ich obecność w internecie jest jeszcze większa, a ich aktywność często się sprowadza się do życia online. Ich sytuacja jest tym poważniejsza, że choć mają ogólną wiedzę o tym, że w internecie istnieją różne niebezpieczeństwa, to jednak uważają, że nie ma skąd czerpać wiedzy, jak sobie z nimi radzić. Rodzice nie są dla nich autorytetem w dziedzinie nowych technologii. Z kolei w szkole, jak podkreślają, lekcje informatyki uczą podstawowej obsługi komputera, czasem programowania.

EDUKACJA CYFROWA

Można przypuszczać, że w przyszłości młodzież będzie lepiej sobie radzić z cyberzagrożeniami, ponieważ już teraz dowiaduje się, że przestrzeń wirtualna może być związana za niebezpieczeństwem. Młodzi ludzie uczą się też na błędach, jak chronić swoją prywatność i rozpoznawać fałszywe komunikaty (choć nie zawsze wiedzą jeszcze, jak to efektywnie robić).

Badani nastolatkowie, którzy uczestniczyli w dodatkowych zajęciach o cyberbezpieczeństwie, oceniają je zwykle jako mało atrakcyjne i mało przydatne.

PODSUMOWANIE



Na ogół nie bagatelizujemy kwestii bezpieczeństwa w sieci. Choć mamy świadomość istnienia różnych cyberzagrożeń, to nie zawsze wiemy, jak się przed nimi chronić. W czasach pandemii tym bardziej powinniśmy uważać na niebezpieczeństwa i z większą ostrożnością dbać o ochronę naszych danych.

Dorośli powinni mieć możliwość systematycznego poznawania nowych zagrożeń online. Przede wszystkim warto stworzyć dla nich zachętę do uczenia się o cyberzagrożeniach oraz pokazywać im te aspekty cyberzagrożeń, które dotyczą bezpośrednio ich życia i mają wpływ na ich dobrostan.

„Nie zapominajmy, że my, obecni dorośli, jesteśmy ostatnim pokoleniem ludzi, którzy urodzili się w czasach, gdy internet nie był tak rozpowszechniony jak obecnie. Nikt nie miał szans nauczyć nas funkcjonowania w świecie, którego jeszcze nie było. Fakt ten nie zwalnia nas – rodziców, nauczycieli, pedagogów - ze wspierania młodego pokolenia w bezpiecznym poznawaniu świata globalnej sieci. To, że młodzi szybciej „klikają", – łatwiej poruszają się w świecie portali, gier i aplikacji – powinno wzbudzić naszą ciekawość. Każdy dorosły, który ma pod opieką „cyfrolatka", powinien wyrazić zainteresowanie nową grą, zadać pytanie o ulubionego youtubera czy najbardziej rozchwytywanego tiktokowca. Najpierw może to wywołać konsternację wśród młodych, ale może też stać się zaczątkiem do rozmowy nie tylko o szkole, ale o świecie, który obecnie dla młodego pokolenia jest równie ważny, co świat realny. Tak jak wcześniejsze pokolenia można było klasyfikować według rodzajów słuchanej muzyki i przynależności do danej subkultury, tak teraz młodych ludzi możemy poznać poprzez obserwację tego, co robią w cyberświecie. Nie musimy grać w gry młodych (chodź osobiście szczerze to polecam) czy oglądać kolejnych „wygibasów" na TikToku. Jeżeli jednak będziemy dziecku, adolescentowi towarzyszyć w jego świecie wirtualnym i traktować jego przestrzeń cyfrową na poważnie, będziemy potrafili ustrzec go przed popełnianiem błędów. Gdyby każda mama czy każdy tata znaleźli czas na obejrzenie zdjęcia, filmiku, które ich dziecko planuje wrzucić do portalu społecznościowego, uchronilibyśmy wielu młodych ludzi przed hejtem czy mową nienawiści. Zmieniają się czasy, zmienia się technika, ale to, co jest stałe i chroni nasze dzieci w sieci, to życzliwa obecność dorosłych w przestrzeni, w której dziecko spędza znaczącą część swojego życia. Kiedyś było to podwórko pod blokiem, dziś jest cyberpodwórko, na którym winniśmy obserwować, z kim bawią się nasze pociechy, od kogo otrzymują informacje lub przez kogo są zapraszane do cyberzabaw."

Wojciech Ronatowicz,
pedagog, nauczyciel, ekspert Forum Bezpiecznego Internetu

Fundacja Kronenberga
citi handlowy
inspiracja
do działania

Fundacja Kronenberga przy Citi Handlowy
ul. R. Traugutta 7/9, 00-067 Warszawa
tel. 22 826 83 24
www.kronenberg.org.pl