

Dziennikarze a bezpieczeństwo w sieci

PressInstitute zbadał, jak dziennikarze, dla których nowe technologie i sieć internetowa są we współczesnym świecie narzędziami codziennej pracy, podchodzą do bezpieczeństwa w sieci.

Czy uważają internet za miejsce bezpieczne? Jaka jest ich świadomość zagrożeń związanych z korzystaniem z internetu? Czy i w jaki sposób dziennikarze dbają o swoje bezpieczeństwo w sieci? Te i inne pytania zadaliśmy dziennikarzom prasowym, internetowym, radiowym i telewizyjnym.

W raporcie prezentujemy wyniki i wnioski z badania

„Dziennikarze a bezpieczeństwo w sieci”.

Partnerem badania i raportu jest mBank, organizator kampanii społecznej dotyczącej bezpieczeństwa w sieci „Uważni w sieci”.

Informacje dotyczące kampanii „Uważni w sieci” są dostępne na stronie mbank.pl/uwazniwsieci

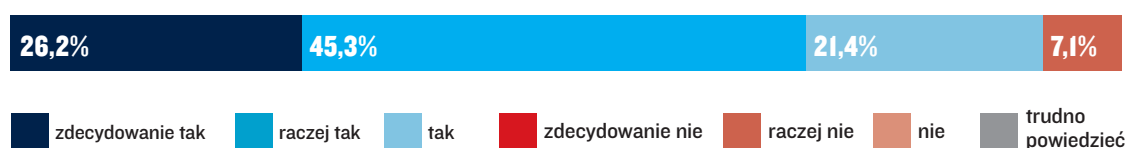
Aż 93 proc. dziennikarzy, którzy wzięli udział w badaniu uważa, że dobrze sobie radzą z nowymi technologiami.

A bezpieczeństwo w sieci?

Zdaniem niemalże 3/4 przebadanych dziennikarzy (72,2 proc.) korzystanie z sieci internetowej jest bezpieczne, ale jedynie 2,4 proc. spośród nich nie obawia się żadnych zagrożeń, jeśli chodzi o korzystanie z internetu. W badaniu respondenci mogli wskazać do trzech zagrożeń, których najbardziej się obawiają. Aż 70,6 proc. wskazało utratę danych w komputerze lub telefonie przez wirusa, 62,7 proc. – włamania na konto bankowe, a 44,4 proc. – przejęcia kontroli nad komputerem. Badani dziennikarze wymienili także inne zagrożenia, a wśród nich najczęściej pojawiały się obawy dotyczące możliwości śledzenia aktywności dziennikarzy w sieci, czy przechwytywania i zbierania danych przez służby specjalne.

CZY DOBRZE SOBIE PAN/I RADZI Z NOWYMI TECHNOLOGIAMI?

(np. urządzenia mobilne z dostępem do sieci, komunikacja w social mediach, chmury itp.)

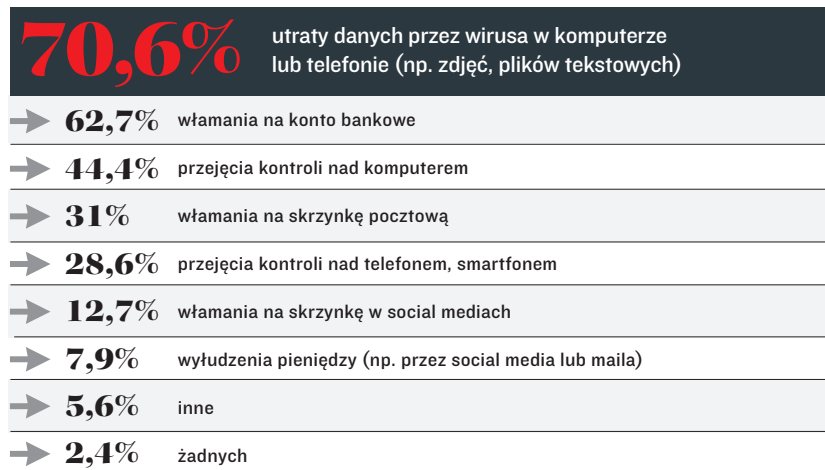


KORZYSTANIE Z SIECI INTERNETOWEJ JEST:



JAKICH ZAGROŻEŃ W SIECI DZIENNIKARZE OBAWIAJĄ SIĘ NAJBARDZIEJ?

Pytanie wielokrotnego wyboru, respondenci mogli wskazać do trzech zagrożeń;
wyniki nie sumują się do 100

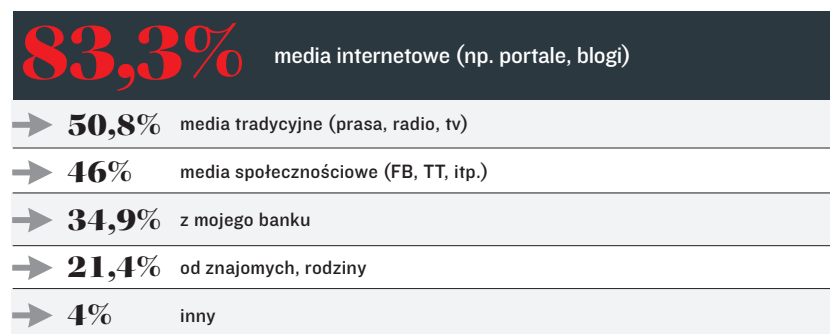


W pytaniu otwartym badani dziennikarze wskazywali jako osoby najbardziej narażone na niebezpieczeństwo w sieci przede wszystkim dzieci, młodzież i seniorów, jako tych najmniej świadomych niebezpieczeństw, jakie niesie za sobą korzystanie z sieci czy – w przypadku osób starszych – najmniej obytych z internetem, a jednocześnie bardziej ufnych. Ale nie tylko. Dziennikarze podkreślali, że wciąż pojawiają się coraz bardziej wyrafinowane sposoby manipulacji i metody np. wyłudzenia danych, co sprawia, że każdy użytkownik internetu jest narażony na ataki cyberprzestępców. Jedynie zdrowy rozsądek, czujność i edukacja mogą ograniczyć ryzyko.

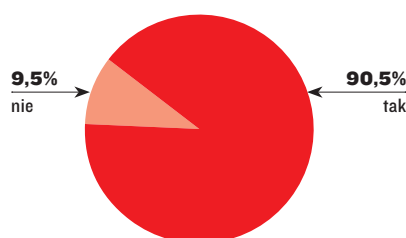
Jak wskazują wyniki badania, dziennikarze zwracają uwagę na informacje i komunikaty o pojawiających się zagrożeniach w sieci. Najczęściej źródłem tych informacji są media internetowe (np. portale, blogi), media tradycyjne i media społecznościowe. Wskazało je odpowiednio: 83,3 proc., 50,8 proc., 46 proc. **Również banki są ważnym źródłem wiedzy o zagrożeniach – wskazało je 34,9 proc. ankietowanych, a czytanie komunikatów bezpieczeństwa banku, w którym respondenci mają konto, deklaruje 90,5 proc.** Ponad połowa (62,7 proc.) czyta te publikowane w serwisie bankowości elektronicznej, a niemalże co piąty – w aplikacji mobilnej (19,8 proc.), a 21,4 proc. – w mailach od banku.

SKĄD CZERPIĄ INFORMACJE O ZAGROŻENIACH W SIECI?

Pytanie wielokrotnego wyboru, wyniki nie sumują się do 100

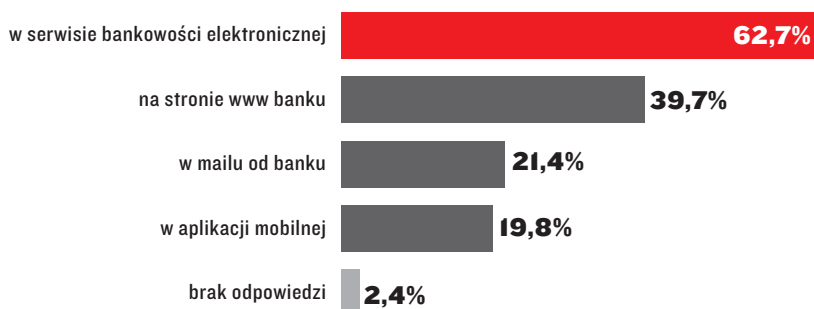


CZY CZYTAJĄ KOMNIKATY BEZPIECZEŃSTWA BANKU, W KTÓRYM MAJĄ KONTO?



GDZIE CZYTAJĄ KOMUNIKATY BEZPIECZEŃSTWA BANKU?

Pytanie wielokrotnego wyboru, wyniki nie sumują się do 100

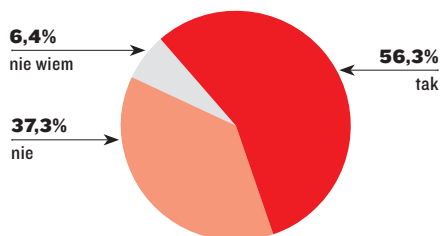


Ponad połowa (56,3 proc.) badanych dziennikarzy miała do czynienia ze szkodliwym oprogramowaniem w swoim komputerze lub w telefonie. I o ile w przypadku komputerów dziennikarze starają się je zabezpieczać, to w przypadku telefonów jest już gorzej. Może to wynikać z przekonania większości badanych (44,4 proc.), że smartfony są mniej podatne na ataki niż komputery.

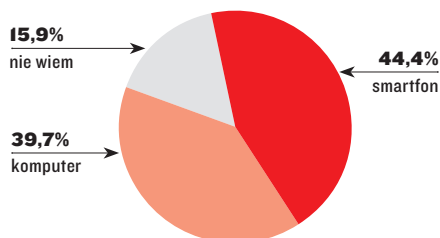
76,2 proc. regularnie aktualizuje oprogramowanie w swoim komputerze, a prawie 90 proc. badanych dziennikarzy korzysta z oprogramowania antywirusowego. Wśród tych, którzy tego nie robią 14,3 proc. przyznaje, że nie wie, jak zainstalować taki program.

Jeśli chodzi o telefony, z których korzystają dziennikarze, to co prawda ich oprogramowanie aktualizuje 71,4 proc. badanych, ale z antywirusów korzysta w tym przypadku tylko 35,7 proc. Ponad połowa (52,3 proc.) nie wie, jak z nich korzystać, a pozostali albo są przekonani, że produkty Apple nie wymagają antywirusów, albo nie ufają tym programom, uważają, że zajmują zbyt dużo pamięci w telefonie lub po prostu odkładają w czasie ich instalację. Z kolei najczęstszym zabezpieczeniem dostępu do telefonu stosowanym przez badanych dziennikarzy jest kod PIN – wskazało go 58,7 proc. osób. Natomiast niemalże połowa (48,4 proc.) po wykryciu szkodliwego oprogramowania w komputerze lub telefonie skanuje urządzenie programem antywirusowym, a co czwarty badany udaje się do serwisu lub informatyka (tylko lub między innymi).

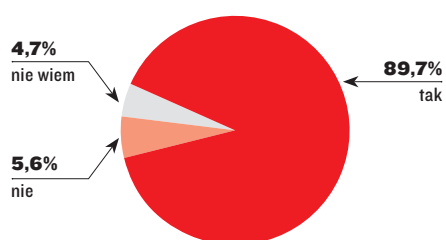
CZY MIELI KONTAKT ZE SZKODLIWYM OPROGRAMOWANIEM W KOMPUPERZE LUB TELEFONIE?



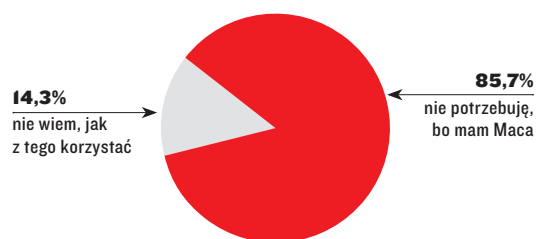
KTÓRE URZĄDZENIE W ODCZUCIU DZIENNIKARZY JEST MNIEJ PODATNE NA ATAKI (NP. WIRUSY)?



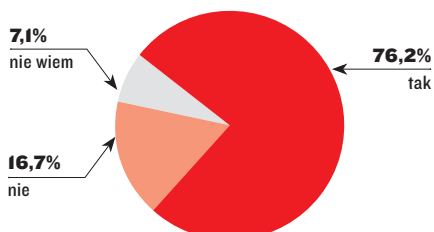
CZY KORZYSTAJĄ Z OPROGRAMOWANIA ANTYWIRUSOWEGO W KOMPUPERZE?



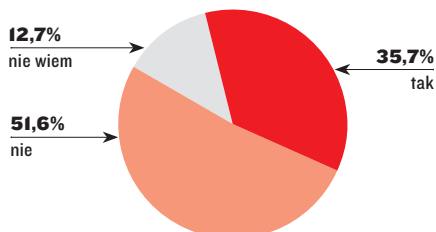
DLACZEGO NIE KORZYSTAJĄ?



CZY NA BIEŻĄCO AKTUALIZUJĄ OPROGRAMOWANIE W KOMPUPERZE?



CZY KORZYSTAJĄ Z OPROGRAMOWANIA ANTYWIRUSOWEGO W TELEFONIE?



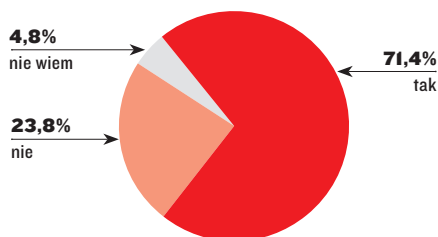
DLACZEGO NIE KORZYSTAJĄ?

→ **32,3%** **nie potrzebuję, bo** zachowuję środki ostrożności, w produktach Apple nie ma potrzeby takich programów, korzystam z iOS, nie mam smartfona, nie ma natywirusów, dla Windows Mobile, wchodzę raczej na bezpieczne, zaufane strony, mam iPhone'a, uważam, że korzystam z telefonu w rozsądny sposób, jak do tej pory brak problemów, nie korzystam z internetu w telefonie

→ **52,3%** **nie wiem, jak z tego korzystać**

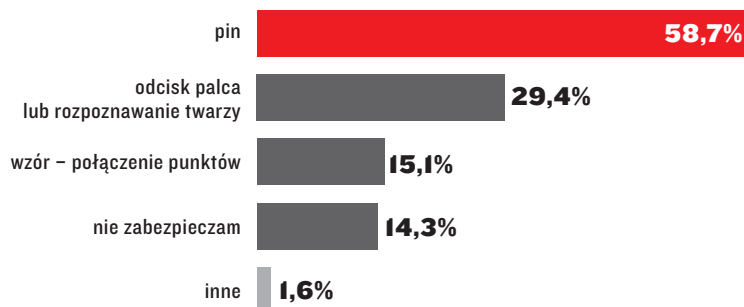
→ **15,4%** **inne (jakie):** nie ufam tym programom, z lenistwa, nie miałam takiej potrzeby, wiem, że powinnam, ale ciągle to odkładam, po tym, co zrobił Kasperski nikomu nie ufam, odkładam w czasie, zbyt obciąża telefon, zżera baterię, nie zdążyłem jeszcze zainstalować, nie mam pamięci na żadne nowe aplikacje

CZY NA BIEŻĄCO AKTUALIZUJĄ SWOJE OPROGRAMOWANIE W TELEFONIE?



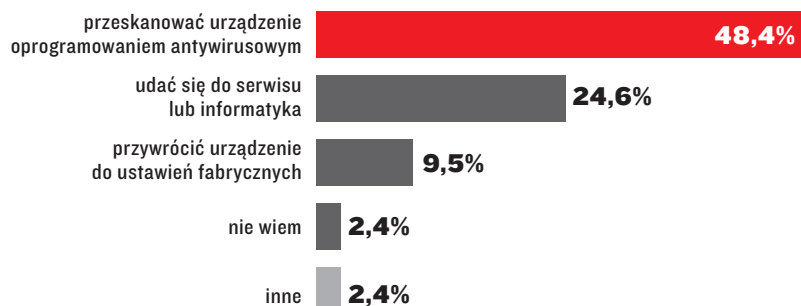
W JAKI SPOSÓB ZABEZPIECZAJĄ SWÓJ TELEFON PRZED NIEPOWOŁANYM DOSTĘPEM?

Pytanie wielokrotnego wyboru, wyniki nie sumują się do 100



**CO TRZEBA ZROBIĆ PO WYKRYCIU SZKODLIWEGO
OPROGRAMOWANIA W KOMPUTERZE LUB TELEFONIE?**

Pytanie wielokrotnego wyboru, wyniki nie sumują się do 100



Wyniki pokazują, że dziennikarze mają większą świadomość zagrożeń bezpieczeństwa od przeciętnego Polaka. Jednak bezpieczeństwo – jak mawia wielu – to proces, czyli potrafi dość często się zmieniać. Ciekawe jest wskazanie smartfona jako najmniej narażonego na ataki. Z punktu widzenia bezpieczeństwa w świecie smartfonów występują problemy, które już dawno zostały względnie dobrze zaadresowane na klasycznych PC-tach. Są to choćby aktualizacje, które szczególnie na platformie Android pozostawiają wiele do życzenia czy programy antywirusowe, które w świecie mobilnym działają często z mocno ograniczonymi możliwościami. Z drugiej strony, dane na smartfonach bywają mniej cenne niż te na klasycznych komputerach, stąd dla atakujących platformy mobilne mogą być celem drugorzędym.

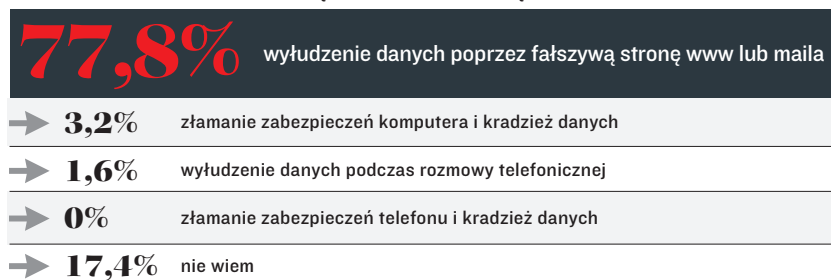
Michał Sajdak
Sekurak.pl

Ponad 3/4 badanych dziennikarzy (77,8 proc.) wskazało prawidłową definicję phishingu. Jednak aż 62,7 proc. badanych dziennikarzy nie zmienia w ogóle haseł do swoich profili w social mediach, a 46 proc. – do poczty elektronicznej. Z kolei 41,3 proc. nie zmienia haseł do kont bankowych, ale także taki sam odsetek robi to jednak raz na kilka miesięcy. 34,9 proc. również raz na kilka miesięcy zmienia je w przypadku profilu na komputerze, co w wielu przypadkach może wynikać z zasad bezpieczeństwa systemu informatycznego pracodawcy.

Tłumaczyć to może dlatego badani za bardziej prawdopodobne uważają wyłudzenie hasła, loginu do swoich prywatnych kont niż tych służbowych, czy bankowych. Do prywatnej skrzynki pocztowej jest możliwe lub nawet bardzo możliwe według 67,5 proc. badanych, do profili w social mediach – 66,6 proc. Natomiast za mało możliwe lub niemożliwe 49,2 proc. uważa wyłudzenie hasła, loginu do konta bankowego, a 41,3 proc. – do służbowej skrzynki pocztowej.

68,2 proc. badanych dziennikarzy korzysta z publicznych sieci WIFI, ale zdają sobie sprawę, że może to być niebezpieczne, bo do swojego konta bankowego nigdy nie loguje się z otwartych sieci np. na lotnisku, czy w restauracji niemalże taki sam odsetek (65,9 proc.).

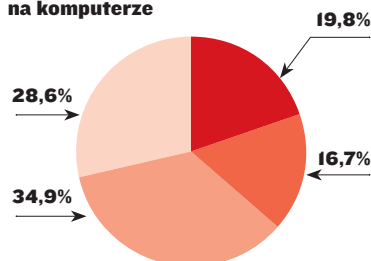
PHISHING TO PODSZYCIE SIĘ POD INSTYTUCJĘ I ...



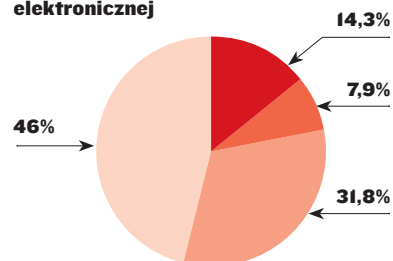
JAK CZĘSTO ZMIENIAJĄ HASŁA DO ...

■ częściej niż raz w m-cu
 ■ co 60dni
 ■ raz na kilka m-cy
 ■ nie zmieniam
 ■ brak odpowiedzi

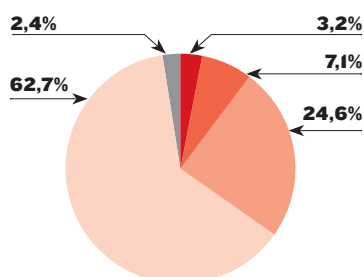
profilu na komputerze



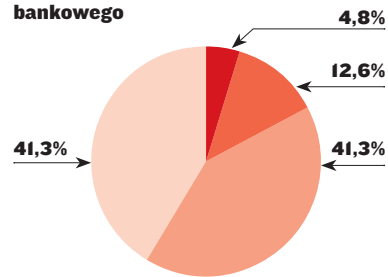
poczty elektronicznej



profilu w social mediach



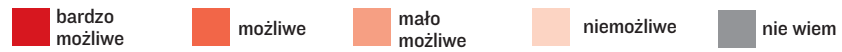
konta bankowego



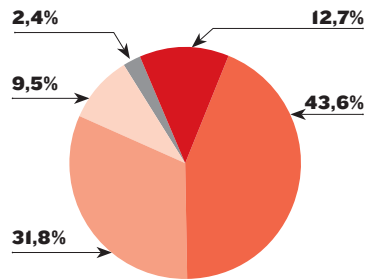
Z jednej strony mamy świadomość różnych zagrożeń, na jakie jesteśmy narażeni, ale z drugiej strony nie przestrzegamy podstawowych zasad bezpieczeństwa. 63 proc. pytanych albo nie zmienia, albo zmienia, ale bardzo rzadko, hasło do profilu w swoim komputerze. 78 proc. również rzadko zmienia hasło do poczty elektronicznej. Jeszcze gorzej chronimy nasze konta w social mediach czy banku. Tymczasem zwykła zmiana hasła (w tym stosowanie odpowiednio trudnego do złamania) to podstawowa rzecz, którą możemy zrobić, by spać spokojnie. Jest to o tyle niepokojące, że większość dziennikarzy ma świadomość, że wyłudzenie loginu i hasła do konta pocztowego, w sieciach społecznościowych czy nawet w banku jest możliwe. Wyniki badania powinna poważnie potraktować kadra kierownicza w mediach i organizować cykliczne szkolenia w zakresie bezpieczeństwa. Każdy specjalista od bezpieczeństwa wie, że najsłabszym ogniwem jest człowiek. Inwestowanie w coraz wymyślniejsze systemy zabezpieczające ma sens wtedy, gdy zabezpieczani nimi np. dziennikarze nie staną się nieświadomymi „końmi trojańskimi”.

Stanisław M. Stanuch

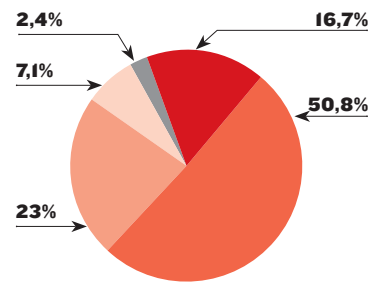
WYŁUDZENIE HASŁA, LOGINU, DANYCH JEST ...



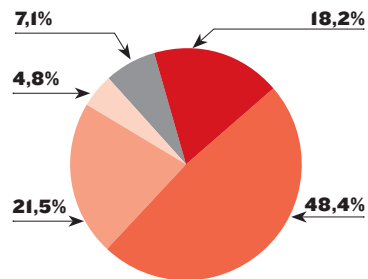
do służbowej skrzynki pocztowej



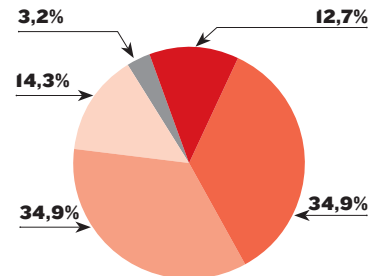
do prywatnej skrzynki pocztowej

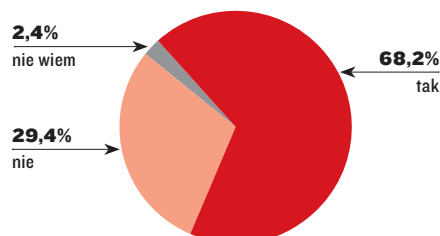
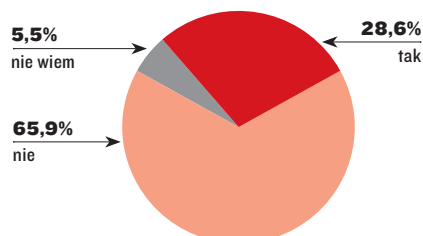


do profilu w social mediach



do konta bankowego



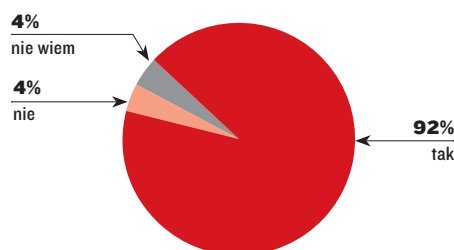
CZY KORZYSTAJĄ Z PUBLICZNYCH SIECI WIFI (NP. NA LOTNISKU, W RESTAURACJI)?**CZY LOGUJĄ SIĘ DO BANKU KORZYSTAJĄC Z PUBLICZNEGO WIFI?**

Ponad 90 proc. zapytanych dziennikarzy twierdzi, że dobrze radzi sobie z nowymi technologiami. Bardzo cieszy fakt, że przedstawiciele mediów śledzą na bieżąco informacje o zagrożeniach w sieci i czytają komunikaty wysyłane przez banki. Wiedza o zagrożeniach płynących z sieci jest jedną z najbardziej skutecznych metod eliminacji tych ryzyk. Zaniepokojenie budzi fakt, że duża grupa dziennikarzy nie korzysta z programów antywirusowych w smartfonach, bezkrytycznie wierzy w bezpieczeństwo jednego systemu operacyjnego a nawet, zdarza się im korzystać z bankowości mobilnej w otwartych sieciach WiFi. Wyniki badania jasno więc wskazują, że nawet osoby zawodowo zajmujące się komunikacją, nie do końca zdają sobie sprawę z zagrożeń jakie niosą ze sobą nowoczesne technologie. Edukacja to wyzwanie, przed którym stajemy my wszyscy – instytucje finansowe, media, jak i sami klienci.

Jarosław Górski
dyrektor departamentu bezpieczeństwa
mBanku

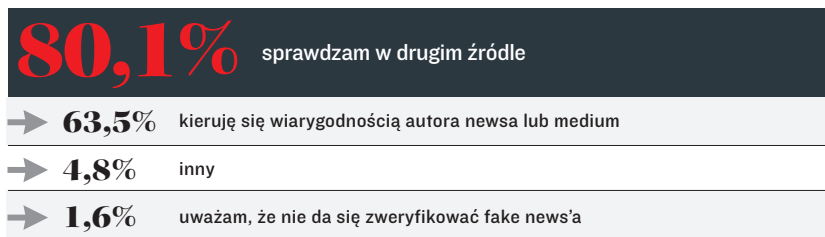
W badaniu dziennikarze odpowiadali również na pytania dotyczące fake news'ów. W przypadku tej grupy zawodowej nie jest zaskoczeniem, że aż 92 proc. badanych dziennikarzy spotkało się z fake news'em. Jedyne 1,6 proc. uważa, że nie da się zweryfikować takiej informacji. 80,1 proc. uważa, że dobrym sposobem na sprawdzenie, czy dana informacja nie jest fake news'em jest sprawdzenie jej w drugim źródle, a 63,5 proc. jest zdania, że jest nim wiarygodność autora informacji lub medium. Dziennikarze podkreślają także, że oprócz researchu i dokładnego sprawdzania źródła informacji, wykorzystują w celu weryfikacji informacji różne aplikacje, media społecznościowe, a także zwracają uwagę na sposób formułowania zdań, czy clickbaitowe tytuły.

CZY MIELI DO CZYNIEŃIA Z FAKE NEWS'EM?



JAK ROZPOZNAJĄ CZY DANA INFORMACJA NIE JEST FAKE NEWS'EM?

Pytanie wielokrotnego wyboru, wyniki nie sumują się do 100

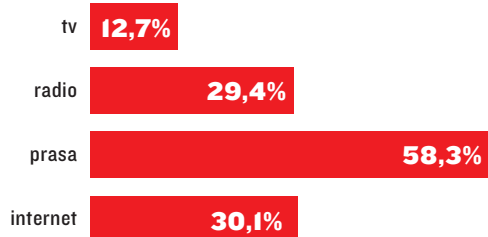


Metryczka



MOJE MIEJSCE PRACY:

Pytanie wielokrotnego wyboru, wyniki nie sumują się do 100



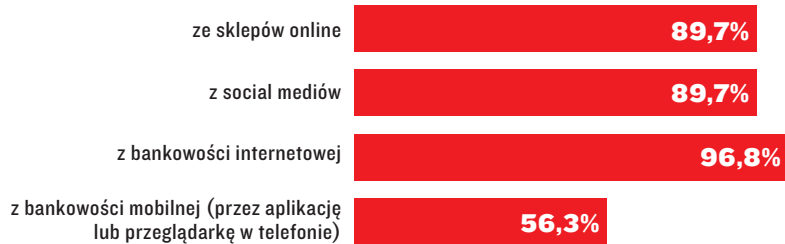
POSIADAM:

Pytanie wielokrotnego wyboru, wyniki nie sumują się do 100



KORZYSTAM:

Pytanie wielokrotnego wyboru, wyniki nie sumują się do 100



Metodologia badania

Badanie „Dziennikarze a bezpieczeństwo w sieci” zostało przeprowadzone metodą CAWI na grupie 126 dziennikarzy ze wszystkich rodzajów mediów, którzy są aktywnymi użytkownikami sieci internetowej zarówno służbowo, jak i prywatnie. Respondenci wypełniali anonimową ankietę online w dn. 10-26 listopada 2017 r.

PressInstitute, CAWI, n=126, 10-26 XI 2017