

KAMPANIA SPOŁECZNA NT. CYBERBEZPIECZEŃSTWA

BADANIE

„Postawy Polaków wobec cyberbezpieczeństwa 2025”

Phishing największym zagrożeniem w przestrzeni cyfrowej!

► TOP 3 najgroźniejszych oszustw w sieci to według badanych:

phishing	kradzież tożsamości	dezinformacja i fake newsy
(z ang.) – aż 88 proc. Polaków za największe zagrożenie w cyfrowym świecie uznaje phishing; respondenci obawiają się, że w wyniku tego oszustwa zostaną wyłudzone ich dane (45 proc.) i pieniądze (43 proc.).	(w tym w social mediach): 38 proc. respondentów uważa atak na wirtualną tożsamość za niebezpieczną.	32 proc. badanych uważa, że zjawisko dezinformacji jest groźne.

Pytanie:

Wskaż obszary, które uważasz obecnie za największe zagrożenia w przestrzeni cyfrowej (możliwość 4 wskazań)



NIE POMAGAJ SIĘ OKRAŚĆ



We wrześniu ruszyła nowa edycja największej w Polsce sektorowej kampanii edukacyjnej „Nie pomagaj się okraść. Zobacz, jak chronić swoje pieniądze”. Przypominamy w niej, że każdy z nas ma realny wpływ na swoje bezpieczeństwo w sieci.

Kampania odsyła zainteresowanych do dedykowanej strony internetowej – www.dbamoswoje.pl, gdzie można znaleźć praktyczne porady dotyczące ochrony danych osobowych, stosowania bezpiecznych haseł oraz unikania oszustw, takich jak phishing.



Dbamo**swoje**

Przewodnik po oszustwach

10 zasad cyberbezpieczeństwa

Bankowy survival

Przydatne linki

Blog

Nie pomagaj się okraść.

Zobacz, jak chronić swoje dane i pieniądze

Przewodnik

Obejrzyj spot



NIE POMAGAJ SIĘ OKRAŚĆ

Celem kampanii jest zwiększenie świadomości społecznej na temat możliwych form wyłudzeń danych osobowych, haseł czy numerów zabezpieczających konta bankowe.



Choć systemy zabezpieczeń stają się coraz bardziej zaawansowane, to wciąż czynnik ludzki bywa najsłabszym ogniwem. Kampania obejmuje spoty telewizyjne, media społecznościowe i działania PR.



EKSPERYMENT SPOŁECZNY

W ramach kampanii przeprowadziliśmy też eksperyment społeczny z fałszywymi reklamami. Na stronie [www.popularnej gazety](http://www.popularnejgazety.pl) zostały zamieszczone banery zachęcające internautów do kliknięcia i zainwestowania kapitału w akcje spółek.



W rzeczywistości służyły one do testowania mechanizmów wyłudzenia danych. Wyniki są alarmujące. W trakcie trzytygodniowej akcji w banery kliknęło **ponad 1,7 miliona internautów**, a zainwestować chciało ponad **8,5 tysiąca użytkowników serwisu www.se.pl**

Zainwestuj

w prestiżowe akcje spółek
z Polski i zagranicy



Zobacz w co inwestują
znani celebryci

Oferta ważna tylko do końca miesiąca

Jaką kwotę chcesz zainwestować?

- ☐ 1 000 zł zarobisz nawet 750 zł
- ☐ 5 000 zł zarobisz nawet 4 000 zł
- ☐ 10 000 zł zarobisz nawet 9 000 zł
- ☐ Więcej niż 10 000 zł zarobisz dużo więcej

ZAZNACZ I WYŚLIJ



PONAD 20 ZNANYCH TWARZY W MAŁEJ KAMPANII

Kampania „Nie pomagaj się okraść” stała się możliwa dzięki małej kampanii „**Bankowcy dla CyberEdukacji**”. W jej ramach powstał cykl krótkich filmów, w których popularni artyści i prezenterzy telewizyjni opowiadają, jak w sposób świadomy, odpowiedzialny i bezpieczny korzystać z dobrodziejstw cyfrowej rzeczywistości.

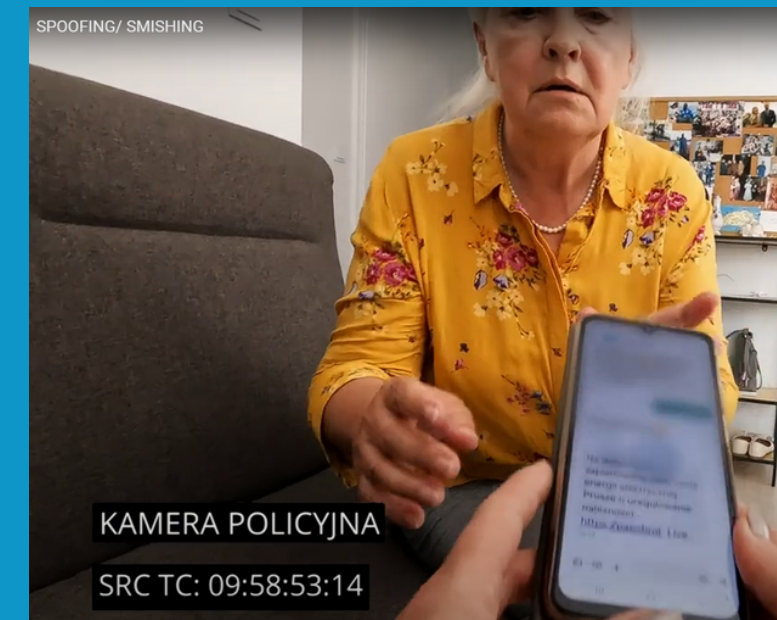
Twarzami kampanii byli m.in.: Beata Tadla, Ewa Kasprzyk, Maciej Orłoś, Jerzy Kryszak, Daria Widawska czy Cezary Pazura. **W tym roku ambasadorami zostali: Tomasz Oświeciński i Olga Bołądź.**



PONAD **120** ODCINKÓW EDUKACYJNYCH* Z UDZIAŁEM BLISKO **100** EKSPERTÓW I ZNANYCH OSÓB



*W tym cykl filmów w konwencji reality opisujących niebezpieczne zjawiska w cyberprzestrzeni, takie jak: **smishing**, **oszustwo na fałszywą inwestycję**, **spoofing** czy **atak z wykorzystaniem socjotechnik**.



DANE CBZC



Działania CBZC w liczbach:

- W 2024 roku przedstawiono zarzuty **1073 osobom**, zatrzymano **około 850 osób**, a **ponad 300** trafiło do aresztu.
- Od stycznia do września 2025 roku zatrzymano **już ponad 850 osób**, a zarzuty karne przedstawiono **1010 podejrzanym** – w przypadku zatrzymań wynik ten przekroczył całoroczne dane z 2024 roku.

Te liczby potwierdzają rosnącą skuteczność operacyjną CBZC w przeciwdziałaniu przestępczości finansowej.

DANE CBZC



Schemat współpracy: Bank ↔ CBZC ↔ Prokuratura

Wymiana informacji w czasie rzeczywistym umożliwia:

- szybkie blokowanie rachunków,
- ograniczanie strat klientów,
- przyspieszenie działań ścigających przestępców.

Krótki apel: współpraca z bankami jest kluczowa dla skuteczności operacyjnej.

ZABEZPIECZONE I ODZYSKANE ŚRODKI



- W 2024 r. zabezpieczono środki finansowe w wysokości **ponad 226 mln zł** oraz odzyskała około **46 mln zł**.
- W 2025 r. zabezpieczono środki finansowe w wysokości **ponad 250 mln zł** oraz odzyskała około **35,5 mln zł**.

To konkretne, wymierne efekty pracy funkcjonariuszy i dowód, że system szybkiego reagowania działa skutecznie.

ZABEZPIECZONE I ODZYSKANE ŚRODKI



Powiązanie zgłoszeń i skuteczności

- Większa liczba zgłoszeń skutkuje wyższą efektywnością działań odzyskiwania środków.
- Apelujemy o systematyczne zgłaszanie oraz zastrzeganie dokumentów w celu zwiększenia bezpieczeństwa finansowego.

Nie wstydź się, reaguj, zgłaszaj!

BADANIE

„Postawy Polaków wobec cyberbezpieczeństwa 2025”

Polacy najczęściej atakowani w social mediach

Pytanie:

Czy w ciągu ostatnich 12 miesięcy spotkałeś/aś się (osobiście lub w Twoim otoczeniu) z następującymi oszustwami? (wielokrotność odpowiedzi)

Ja lub ktoś w moim otoczeniu miał do czynienia ze zhakowaniem konta w mediach społecznościowych (przejęcie konta i wizerunku)

22%

Ja lub ktoś w moim otoczeniu miał do czynienia z phishingiem, czyli z próbą kradzieży danych osobowych/poufnych informacji i/lub środków pieniężnych za pośrednictwem fałszywych emaili, stron www, SMS-ów czy komunikatorów

21%

Ja lub ktoś w moim otoczeniu miał do czynienia z oszustwem dokonany telefonicznie – oszust podszywał się pod firmę, instytucję, urząd bądź osobę (oszustwa typu vishing i spoofing)

17%

Ja lub ktoś w moim otoczeniu miał do czynienia z oszustwem inwestycyjnym dokonany za pośrednictwem rozmowy telefonicznej z fałszywym doradcą

12%

Ja lub ktoś w moim otoczeniu miał do czynienia z malware, czyli złośliwym oprogramowaniem, którego celem jest uszkodzenie, zakłócenie działania lub uzyskanie nieautoryzowanego dostępu do komputera/smartfona

9%

Ja lub ktoś w moim otoczeniu miał do czynienia z oszustwem inwestycyjnym dokonany za pośrednictwem fałszywej reklamy wygenerowanej przez sztuczną inteligencję (tzw. deepfake)

9%

Ja lub ktoś w moim otoczeniu miał do czynienia z tzw. oszustwem romantycznym, czyli poprzez nawiązanie relacji na portalu randkowym czy w social mediach (oszust udawał relację, aby wyłudzić pieniądze)

7%

Nie pamiętam, abym miał/a styczność z którąkolwiek z tych metod oszustw

44%

Polacy wskazali dezinformację i fake newsy jako 3. największe zagrożenie w sieci, ale zbyt rzadko je zgłaszają

Pytanie:

Jakie sposoby Twoim zdaniem są najlepszą ochroną przed skutkami dezinformacji lub fake newsów?

(możliwość 3 wskazań)

Nie traktuję mediów społecznościowych jako głównego źródła wiedzy

38%

Czytam całą informację, a nie tylko nagłówki

34%

Weryfikuję informacje w kilku źródłach różnego pochodzenia

31%

Nie udostępniam treści, których pochodzenia nie sprawdziłem/am

27%

Ufam głównie informacjom z wiarygodnych krajowych źródeł

24%

Nie ulegam presji czasu przy czytaniu informacji

23%

Zgłaszam/blokuję treści o wątpliwym pochodzeniu

17%

Sprawdzam pochodzenie zdjęć/obrazów ilustrujących informację

16%

Ufam głównie informacjom z wiarygodnych zagranicznych źródeł

11%

Nie wiem, co jest najlepszą ochroną przed skutkami dezinformacji lub fake newsów

5%

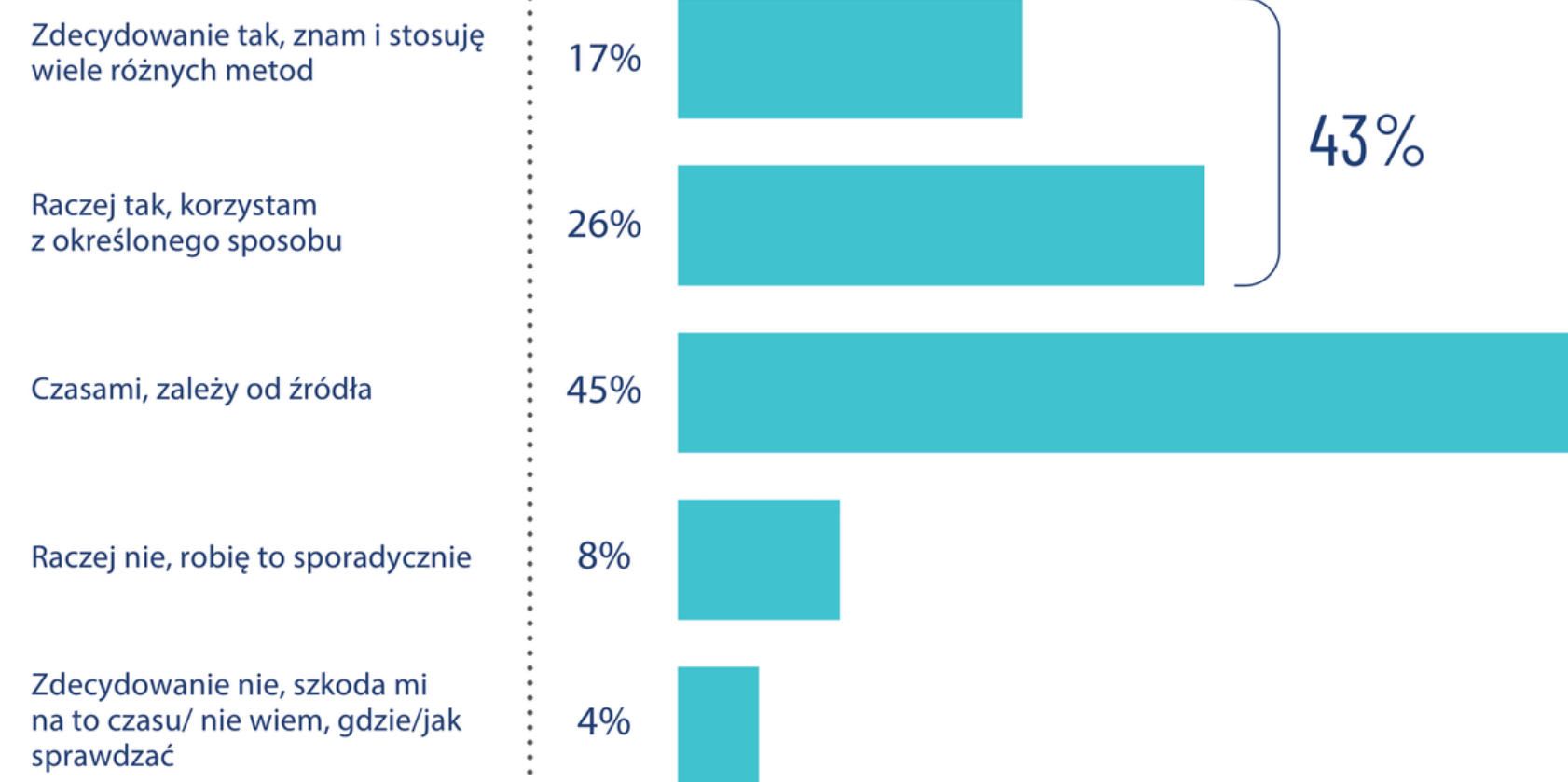
BADANIE

„Postawy Polaków wobec cyberbezpieczeństwa 2025”

Niestety mniej niż połowa Polaków regularnie weryfikuje informacje pojawiające się w Internecie

Pytanie:

Czy w jakikolwiek sposób sprawdzasz wiarygodność informacji, które przeczytałeś/aś w Internecie? (jedno wskazanie)

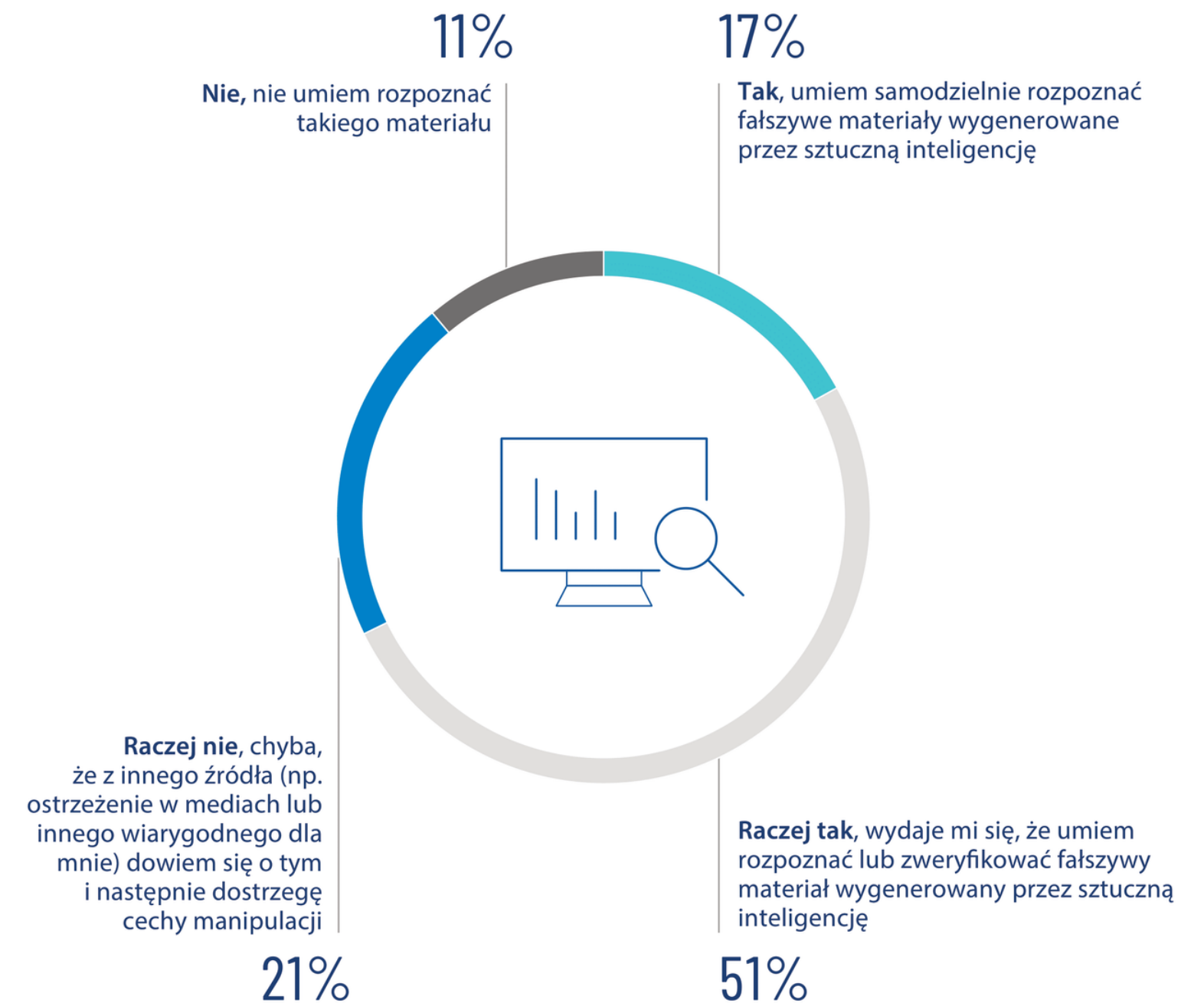


BADANIE
„Postawy Polaków wobec cyberbezpieczeństwa 2025”

Ponad połowie Polaków wydaje się, że potrafią rozpoznać deepfake'i

Pytanie:

Czy umiesz rozpoznać tzw. deepfake, czyli nieprawdziwe materiały audiowizualne (fałszywe nagrania i zdjęcia) wytworzone przy użyciu technik sztucznej inteligencji? – deepfake'i wykorzystywane są m.in. do oszustw finansowych, dyskredytowania osób publicznych, rozprzestrzeniania dezinformacji. (jedno wskazanie)



DZIĘKUJEMY ZA UWAGĘ

ZAPRASZAMY DO KONTAKTU

Związek Banków Polskich
ul. Kruczkowskiego 8
00-380 Warszawa



zbp.pl



dr Przemysław Barbrich
Dyrektor Komunikacji i PR
tel. 660 763 831



ZWIĄZEK
BANKÓW
POLSKICH