Konwent na rzecz Współpracy i Rozwoju
Polskiej Bankowości Spółdzielczej 2024

Cyberbezpieczeństwo w dobie współczesnych zagrożeń

dr Jarosław Biegański
FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP

Warszawa, 18 stycznia 2024

REKLAMY FAŁSZYWYCH INWESTYCJI

Źródło: BREBYTES

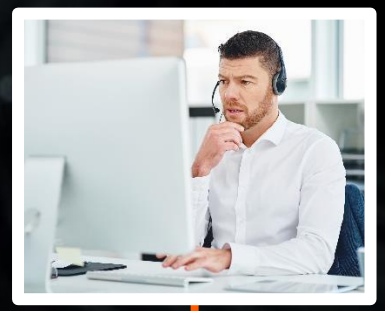
SPOOFING - VOICE PHISHING –

OSZUSTWO, KTÓRE NIE SŁABNIE NA SILE

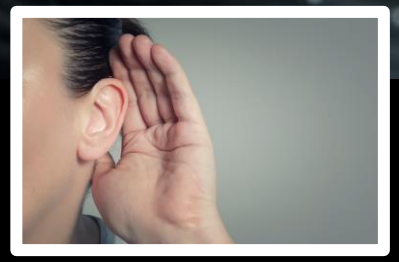
Do osoby fizycznej dzwoni

osoba podająca się za pracownika

Departamentu Bezpieczeństwa Banku (ZBP, KNF itp.) ….



1. Zna imię i nazwisko osoby do której dzwoni



2. Na telefonie ofiary wyświetla się nr infolinii banku

3. Pyta czy dana osoba potwierdza rzekomy przelew, kredyt, logowanie z poza terenu Polski, którego „de facto” nie było

4. Ofiara oczywiście zaprzecza

5. W tym momencie konsultant-przestępca informuje, iż dana osoba ma zainfekowany telefon i konieczne jest jego sprawdzenie

6. W związku z powyższym nakłania rozmówcę do instalacji programu ze sklepu GooglePlay, który rzekomo ma zdiagnozować zagrożenie, a w rzeczywistości służy do zdalnego nadzoru nad telefonem

7. Po instalacji, najczęściej programu ANYDESK, oszuści przejmują kontrolę nad telefonem ofiary (ostatnio Teams z funkcją dzielenia ekranu)

FINCERT.PL ISAC BANKOWE CENTRUM CYBERBEZPIECZEŃSTWA

Gra edukacyjna
- jako skuteczne narzędzie komunikacji ostrzeżeń do klientów

1

Zamieszczenie na stronach Super Expressu banerów z kuszącą ofertą kupna produktów po atrakcyjnych cenach

2

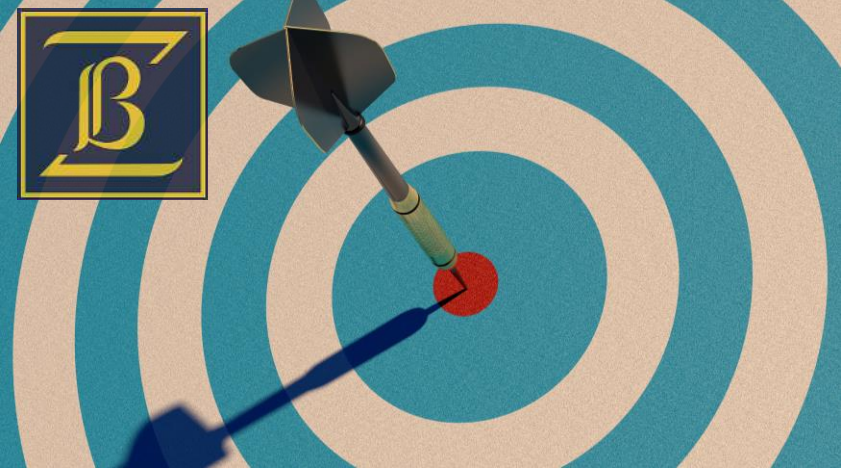
Pozyskanie potencjalnych klientów i uzyskanie od nich dorozumianej zgody na przekazanie danych wrażliwych

3

Emisja filmu edukacyjnego ilustrującego w jaki sposób dane wrażliwe klienta mogły trafić w ręce przestępców i jak mogły być wykorzystane

Zob. film „Uwaga – to nie jest gra to jest prawdziwe życie”

Projekt realizowany przez ZBP wspólnie z Komendą Główną Policji i dziennikiem Super Express



Podsumowanie wyników GRY EDUKACYJNEJ

- ✓ W ciągu 14 dni ponad 14 tysięcy osób kliknęło w fałszywe banery i było gotowych podzielić się swoimi wrażliwymi danymi, aby skorzystać z oferty!
- ✓ Klienci zaufali reklamie i kliknęli w formatkę w celu udostępnienia swoich danych
- ✓ Każda z tych osób mogła być potencjalną ofiarą przestępców i utracić swoje oszczędności

EKSPERYMENT SPOŁECZNY – PUBLIKACJE PRASOWE

Publikacja w drukowanym wydaniu Super Expressu z dnia 14 grudnia 2023 r.

Cyberprzestępcy czyhają na ciebie w internecie

BĄDŹ CZUJNY W SIECI

Internet to miejsce, z którego korzystamy codziennie. Zostawiamy swoje dane osobowe, pobieramy różnego rodzaju pliki, wysyłamy wiadomości, używamy mediów społecznościowych i korzystamy z bankowości. Jednak internet to też miejsce, w którym może czyhać na nas niebezpieczeństwo.

Z badania „Postawy Polaków wobec cyberbezpieczeństwa" dla Fundacji Warszawski Instytut Bankowości wynika, że 71 proc. Polaków czuje się bezpiecznie korzystając z bankowości elektronicznej. 67 proc. Polaków korzysta z usług urzędów i banków wyłącznie online, a 57 proc. uznaje banki jako liderów w zakresie cyberbezpieczeństwa. Polacy (71 proc.) uważają, że banki w obszarze cyberbezpieczeństwa stosują wysokie standardy i raczej czują się spokojni o bezpieczeństwo zgromadzonych oszczędności.

Odczucia i opinie to jedno, inną prawą są metody stosowane przez cyberprzestępców. A na to może dać się złapać praktycznie każdy. Co zatem zrobić? O czym pamiętać w ferworze przedświątecznych zakupów? Najważniejszych jest kilka „cyber" zasad.

1. Chroń swoje dane osobowe!

Ludzie często świadomie pokazują zbyt wiele w internecie, a czasem po prostu chwalą się np. zdanym prawem jazdy lub nowym dowodem. W ten sposób złodzieje bardzo szybko mogą poznać numer PESEL, adres zamieszkania i inne dane. Zastanów się dwa razy nad tym, co publikujesz w sieci i nie pomagaj cyberprzestępcom,

2. Stosuj programy antywirusowe

Nigdy nie wiesz kiedy możesz stać się ofiarą cyberataku. Zabezpiecz swoje urządzenia elektroniczne antywirusem i bądź o krok do przodu przed oszustami.

3. Zawsze ustawiaj silne hasła!

Tworząc hasło pamiętaj, aby było ono silne, długie i oparte o skojarzenia, liczby i znaki specjalne. Posiadanie silnego hasła ma sens, dopóki będziesz pamiętał o wylogowaniu! Ta czynność po zakończeniu pracy z danym systemem, aplikacją lub usługą powinno być twoim naturalnym odruchem.

4. Sprawdzaj bezpieczeństwo stron, z których korzystasz

Kupując w sklepach internetowych sprawdzaj, czy mają szyfrowane połączenie oznaczone kłódką i odpowiednim certyfikatem. Płać tylko z własnego komputera lub telefonu. Zanim wejdz na nieznaną ci stronę internetową, upewni że jest ona bezpieczna. Możesz w tym celu wbudowanych narzędzi bezpieczeństwa prz darek internetowych, jednak najlepiej zast dodatkowo zewnętrzne narzędzie do spraw nia witryn. Warto również zweryfikowa strona posiada certyfikat https. Chodzi o t bezpieczeństwo, dlatego pamiętaj – podejr strony i linki to także źródło wirusów.

5. Nigdy nie otwieraj wiadomo i dołączonych do nich załącz ków z nieznanych źródeł

Zawsze weryfikuj linki, które chcesz otwo i upewnij się, że wiesz, dokąd one zaprowa Najedź myszką na dowolny link, aby zw fikować adres URL, z którym jest napra powiązany. To właśnie w załącznikach m być ukryte złośliwe oprogramowania i wi

6. Zawsze twórz kopię zapasowe!

Tworzenie kopii zapasowej danych, czyli tzw. „backup", to nic innego jak dodatkowe zabezpieczenie twoich plików. Służy ono do odtworzenia oryginalnych danych w przypadku ich utraty bądź uszkodzenia. DK

Więcej: www.bankiwpolsce.pl/cyberbezpieczenstwo

PAMIĘTAJ! Cyberprzestępcy będą grać na emocjach oraz będą manipulować. Nie daj się zwieść. Wszystko sprawdzaj, bądź czujny w sieci.

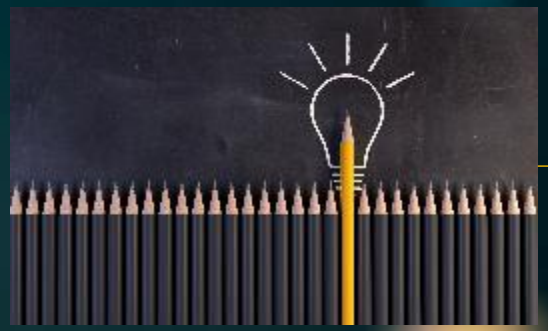
Na zakończenie eksperymentu AKCJA została opisana w drukowanym wydaniu Super Expressu w nakładzie ok. 100 000 egzemplarzy i wraz z poradnikiem jak dbać o cyberbezpieczeństwo przekazana czytelnikom w przyjaznej graficznej formie

Inne działania edukacyjne

WSPÓLNE PRZEDSIĘWZIĘCIE Z TV PULS

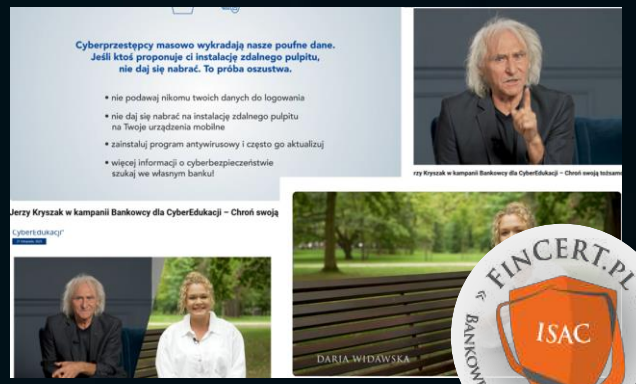
Współuczestnictwo w kampanii telewizyjnej TV Puls poprzez objęcie patronatem Związku Banków Polskich ogólnopolskiej kampanii społecznej na rzecz bezpieczeństwa seniorów.

Cyber-edukacja klientów



DZIALANIA EDUKACYJNE WOBEC KLIENTÓW: KOMUNIKATY, WYSTĄPIENIA - KONFERENCJE PRASOWE ZBP, FILMY EDUKACYJNE

- Komunikaty i ostrzeżenia realizowane przez ZBP wspólnie z Policją - publikowane na stronach Policji, ZBP i wykorzystywane przez banki
- Komunikaty informują o aktualnych zagrożeniach dla klientów korzystających ze zdalnych usług i produktów bankowych i jednocześnie zawierają zalecenia, jak bezpiecznie korzystać z usług świadczonych przez banki za pośrednictwem bankowości internatowej, mobilnej i kartowej
- Lista komunikatów i ostrzeżeń dostępna na stronie FinCERT.pl
- „Bankowcy dla CyberEdukacji" cykl filmów z udziałem popularnych osób o tematyce związanej z cyberbezpieczeństwem klientów banków
- w przygotowaniu: filmy w formacie paradokumentu, które skupią się na cyberprzestępstwach poprzez pryzmat osób oszukanych



Cyber-edukacja ekspercka

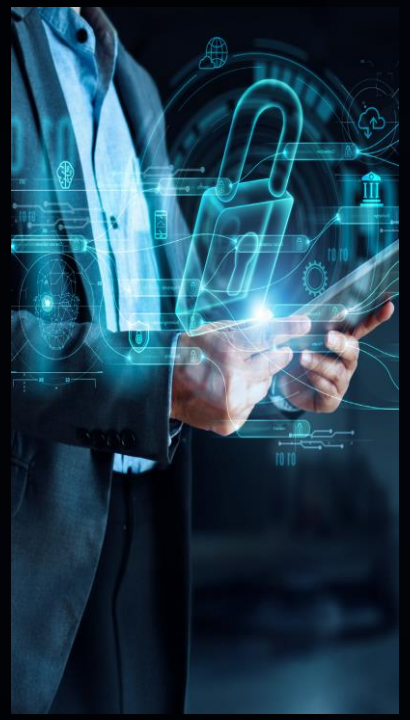
WARSZTATY I SZKOLENIA EKSPERCKIE

- **Posiedzenia trzech forów – Forum Bezpieczeństwa Transakcji Elektronicznych, Forum Bezpieczeństwa Transakcji Kartowych, Forum Threat Intelligence**
- **Uczestnictwo w Grupach Operacyjnych**
- **Wymiana informacji za pośrednictwem międzybankowych systemów służących do wymiany informacji**
- **Zamknięte wydarzenia:**
  - warsztaty szkoleniowe banków i policji (CBZC) z obszaru cyberbezpieczeństwa w Jakuszycach i Białowieży;
  - wyjazdowe posiedzenia Forum AML RBB ZBP w Serocku;
  - konferencja naukowa: **Przestępczość teleinformatyczna XXI w.** Akademii Marynarki Wojennej w Gdyni;
- **Otwarte wydarzenia - ogólnopolskie konferencje naukowe:**
  - Europejski Kongres Finansowy w Sopocie;
  - Forum Bezpieczeństwa Banków w Warszawie;
  - Konferencja antyfraudowa RBB „Bankówka”;
  - Konferencja SafeBank – Ochrona tożsamości – czy umiemy i możemy chronić tożsamość naszych klientów;
  - Forum Technologii Bankowości Spółdzielczej 2023.
- **Studia podyplomowe: „Przeciwdziałanie cyberprzestępczości finansowej” – inicjatywa Uniwersytetu WSB Merito w Poznaniu - AMW w Gdyni - ZBP**

Regulacje prawne wpływające na cyberbezpieczeństwo banków i ich klientów

- ustawa z dnia 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczenia skutków kradzieży tożsamości (Dz. U. z 2023 r. poz. 1394).
- ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2023 r. poz. 1703).
- Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz.U. 2023 poz. 1234)

Rekomendacje Zarządu Związku Banków Polskich opublikowane lub zaktualizowane w 2023 r.



3 października 2023 r.

- Rekomendacje dot. obsługi klientów, którzy angażują środki w oszukańcze inwestycje w kryptoaktywa lub na rynku FOREX
- Rekomendacje dot. ochrony pracowników banków, których dane zostały wykorzystane przez sprawców przestępstw podszywających się pod nich podczas rozmów telefonicznych z klientami banku

24 października 2023 r.

- Rekomendacje dot. algorytmów postępowania organów ścigania w przypadku ujawnienia zdarzeń dotyczących kart płatniczych
- Rekomendacje dotyczące przeciwdziałania atakom logicznym na infrastrukturę bankomatową

30 listopada 2023 r.

- Rekomendacje sektora bankowego dotyczące przeciwdziałania transakcjom oszukańczym

Wnioski płynące z analiz zdarzeń prowadzonych przez FinCERT.pl – BCC ZBP

- Najpoważniejsze szkody wyrządzają incydenty, w których do płatności dochodzi z wykorzystaniem silnego uwierzytelnienia (SCA)
- Pokrzywdzony często świadomie udostępnia dane uwierzytelniające
- Zmanipulowany klient sam inicjuje płatność na własną szkodę

Dziękuję za uwagę

FinCERT.pl
– Bankowe Centrum Cyberbezpieczeństwa
ZBP

kontakt:
bcc@zbp.pl
alert@fincert.pl