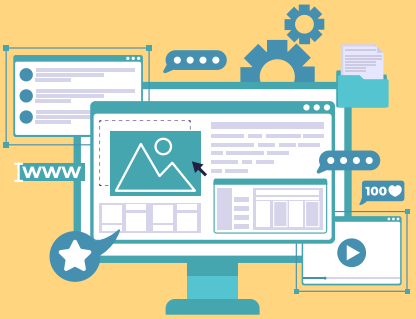
USTAL Z BABCIĄ HASŁO

ATAKI SOCJOTECHNICZNE I PHISHING



1 DEFINICJA

To metoda manipulacji, która wykorzystuje ludzkie słabości, aby nakłonić ofiarę do wykonania określonego działania, tj. ujawnienia danych osobowych i/ lub finansowych, z wykorzystaniem technologii oraz AI.

2 EMOCJE

Oszuści często grają na emocjach takich jak strach, ciekawość, współczucie czy chęć pomocy. Mogą np. przesyłać alarmujące wiadomości o rzekomym zagrożeniu lub konieczności pilnego działania.

3 PROFIL OSZUSTA

Atakujący mogą podszywać się pod zaufane osoby lub instytucje (np. pracowników banku, urzędników, przyjaciół) i używać znanych, wiarygodnych nazwisk czy logo.

4 PLAN DZIAŁANIA OSZUSTA

Przestępcy mogą wcześniej zebrać informacje o ofierze, korzystając z mediów społecznościowych, co pozwala im na lepsze dopasowanie swoich ataków i wzbudzenie większego zaufania.

PRZYKŁADY

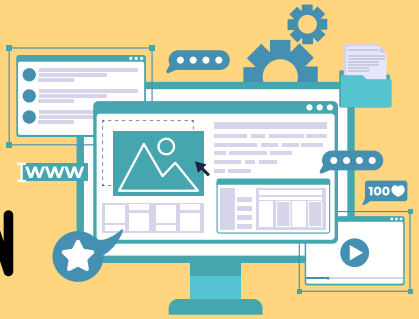
- fałszywe strony Internetowe sklepów
- prośby o wpłaty na poszkodowanych, biednych, zwierzęta porzucone w schroniaskach

5

- SMS ponaglające do dopłaty do paczki od kuriera (wraz z linkiem)
- e-maile lub wiadomości SMS, które wyglądają jak komunikaty z banku lub od dystrybutorów prądu i gazu (wraz z linkiem)
- telefon z banku lub Policji
- „darmowe” prezenty lub nagrody w Internecie

USTAL Z BABCIĄ HASŁO

ATAK SOCJOTECHNICZNY PRZEZ TELEFON



METODA "NA WNUCZKA"

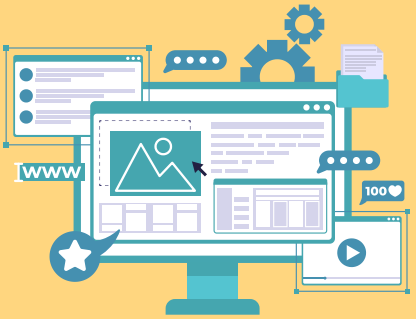
- Oszust kontaktuje się z ofiarą, twierdząc, że jest jej wnuczkiem lub innym członkiem rodziny. Rozmowę rozpoczyna od słów: "Cześć Babciu/ Dziadku" a potem milknie po to by usłyszeć odpowiedź na przywitanie z użyciem imienia wnuczka.
- Przykłady: telefon od „wnuczka" informującego o wypadku samochodowym, prośba o pomoc w zapłaceniu kaucji czy rzekomych kosztów leczenia.
- W komunikatach od „wnuczków" często pojawia się presja czasu, oszuści mówią, że trzeba działać „pilnie", „natychmiast", „nie można z tym czekać".
- Ofiara jest proszona o przesłanie pieniędzy lub wykonanie przelewu na konto, aby „pomóc" bliskiej osobie. Przestępca może podać fałszywe dane kontaktowe lub numer konta.
- Jeśli otrzymasz nagły telefon, w którym ktoś domaga się pilnego działania lub podania danych osobowych, nie reaguj natychmiastowo. Zawsze daj sobie czas na przemyślenie sytuacji. Zadzwoń też do bliskiej osoby i opowiedz o zdarzeniu. Taka rozmowa może pomóc Ci poradzić sobie z problemem.

#USTAL Z BABCIĄ HASŁO

- Oszuści często blokują linię telefoniczną aby utrunić ofierze skontaktowanie się z rodziną, w tym z osobą, której telefon dotyczył. Bądź więc cierpliwy jeśli "wnuczek" nie odbiera telefonu.

USTAL Z BABCIĄ HASŁO

ĆWICZENIE



1 ROLA NAUCZYCIELA

Przygotowanie wydruków treści fałszywych maili i SMS, które mogłyby zostać wykorzystane do ataków phishingowych.

Podział uczniów na grupy 2-4 os.

Czuwanie nad czasem pracy uczniów i prawidłowym przebiegiem zadania, a następnie jego podsumowanie.

2 ROLA UCZNIA

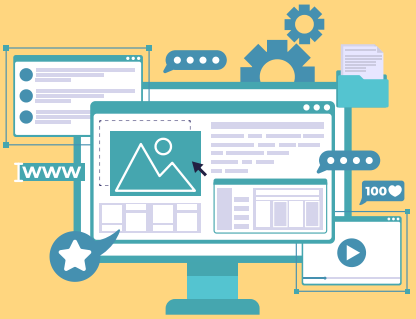
Analiza przykładów treści fałszywych e-maili i SMS oraz zaznaczenie elementów, które wzbudzają podejrzenia.

Powtórzenie ćwiczenia z dowolną osobą starszą.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

ĆWICZENIE



E-MAIL NR 1

Temat: „Pilne: Twoje konto zostało zablokowane!”
Treść: „Ze względów bezpieczeństwa Twoje konto zostało czasowo zablokowane. Aby je odblokować, kliknij poniższy link i zaloguj się”.

E-MAIL NR 2

Temat: „Problem z ostatnią płatnością”.
Treść: „Nie mogliśmy przetworzyć Twojej ostatniej transakcji. Prosimy zaktualizować dane swojego konta, klikając poniżej”.

E-MAIL NR 3

Temat: „Gratulacje! Wygrałeś iPhone’a!”
Treść: „Wygrałeś iPhone'a w naszym losowaniu! Kliknij tutaj, aby odebrać swoją nagrodę”.

E-MAIL NR 4

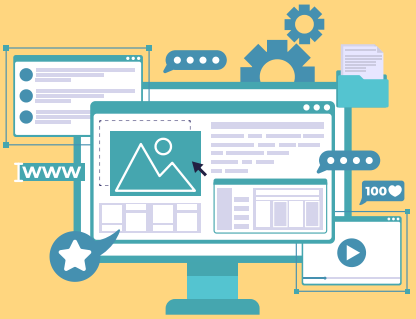
Temat: „Twoje konto zostanie zamknięte!”
Treść: „Nie udało nam się odnowić subskrypcji Twojego konta. Aby uniknąć zamknięcia, zaloguj się tutaj i zaktualizuj informacje”.

#USTAL Z BABCIĄ HASŁO

źródło: https://www.szkolalukawiec.pl/start/index.php/szkola-miedzypokoleniowa/zajecia-5-phishing-i-metoda-na-wnuczka

USTAL Z BABCIĄ HASŁO

ĆWICZENIE



SMS NR 1

Temat: „Podejrzana aktywność na koncie bankowym”
Treść: „Twoje konto bankowe zostało zablokowane z powodu podejrzanej aktywności. Kliknij tutaj, aby potwierdzić swoje dane: [złośliwy link]”

SMS NR 2

Temat: „Nagroda lub wygrana”
Treść: „Gratulacje! Wygrałeś nagrodę w wysokości 5000 zł. Kliknij tutaj, aby odebrać swoją wygraną: [złośliwy link]”

SMS NR 3

Temat: „Potwierdzenie dostawy paczki”
Treść: „Twoja paczka nie mogła zostać dostarczona. Kliknij tutaj, aby zaktualizować informacje o dostawie: [złośliwy link]”

SMS NR 4

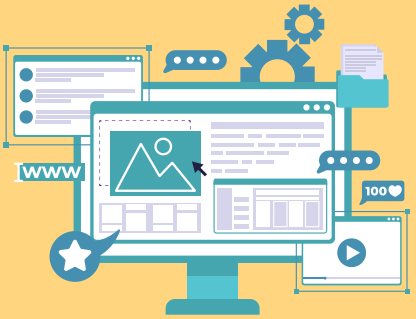
Temat: „Aktualizacja konta bankowego”
Treść: „Aktualizacja konta bankowego jest wymagana. Kliknij tutaj, aby zaktualizować swoje dane: [złośliwy link]”

#USTAL Z BABCIĄ HASŁO

źródło: https://www.szkolalukawiec.pl/start/index.php/szkola-miedzypokoleniowa/zajecia-5-phishing-i-metoda-na-wnuczka

USTAL Z BABCIĄ HASŁO

ĆWICZENIE



SMS NR 5

Temat: „Problemy z płatnością”
Treść: „Nie udało się przetworzyć płatności na twoim koncie. Kliknij tutaj, aby potwierdzić dane karty kredytowej: [złośliwy link]”

SMS NR 6

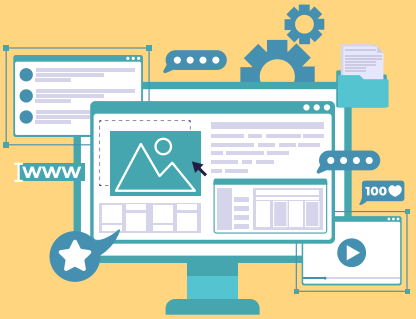
Temat: „Ostrzeżenie o wirusie”
Treść: „Twój telefon jest zainfekowany wirusem! Kliknij tutaj, aby natychmiast usunąć zagrożenie: [złośliwy link]”

#USTAL Z BABCIĄ HASŁO

źródło: https://www.szkolalukawiec.pl/start/index.php/szkola-miedzypokoleniowa/zajecia-5-phishing-i-metoda-na-wnuczka

USTAL Z BABCIĄ HASŁO

JAK ROZPOZNAĆ ATAK PHISHINGOWY



NIEZNANY NADAWCA:

Jeśli otrzymasz e-mail od nieznanej osoby lub organizacji, zawsze bądź ostrożny.

PODEJRZANY TEMAT:

E-maile phishingowe często mają tematy, które wywołują poczucie pilności, takie jak „Twoje konto zostanie zablokowane” lub „Pilna aktualizacja konta”.

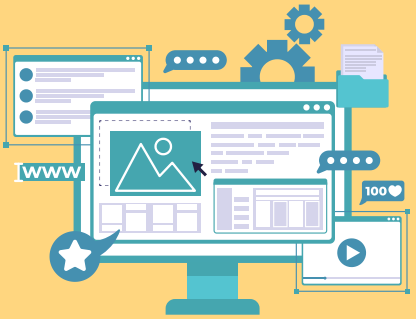
PODEJRZANE LINKI I ZAŁĄCZNIKI:

Nigdy nie klikaj linków ani nie otwieraj załączników w podejrzanych e-mailach. Mogą one prowadzić do złośliwych stron lub zawierać złośliwe oprogramowanie.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

JAK ROZPOZNAĆ ATAK PHISHINGOWY



LITERÓWKI I BŁĘDY GRAMATYCZNE:

Fałszywe e-maile często zawierają literówki, błędy ortograficzne i gramatyczne, np. info@bank.com może być zmienione na info@b4nk.com).

PROŚBY O WRAŻLIWE INFORMACJE:

Nigdy nie podawaj danych osobowych, numerów kont, haseł ani kodów CVV z karty kredytowej w odpowiedzi na e-mail.

ZGŁOŚ PHISHINGOWY E-MAIL:

Zgłoś e-mail do CERT Polska (zespołu działającego w strukturach NASK do reagowania na incydenty cyberataków), aby pomóc w walce z phishingiem w Polsce. Możesz to zrobić, przesyłając e-mail na adres cert@cert.pl.

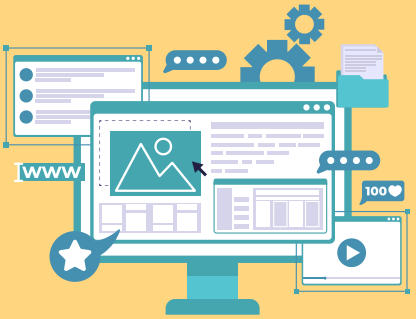
USUŃ E-MAIL:

Po zgłoszeniu phishingowego e-maila usuń go ze swojej skrzynki odbiorczej.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

JAK ROZPOZNAĆ ATAK PHISHINGOWY



Przestępcy nieustannie modyfikują scenariusze swoich działań!

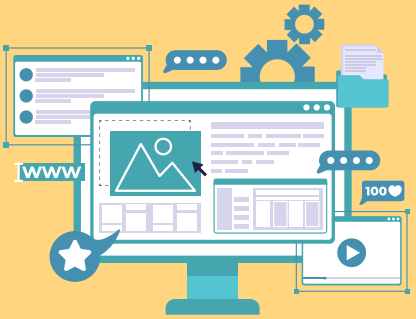
CO ZROBIĆ W PRZYPADKU OTRZYMANIA SMS-A PHISHINGOWEGO:

- NIE klikaj w linki zawarte w podejrzanych SMSach.
- Nie odpowiadaj na podejrzane wiadomości tekstowe.
- Zgłoś SMS swojemu operatorowi sieci komórkowej oraz odpowiednim służbom.
- Usuń podejrzaną wiadomość tekstową ze swojego telefonu.
- Poinformuj bliskie osoby o otrzymaniu takiego SMS-a, aby były świadome zagrożenia.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

JAK STWORZYĆ "SILNE" HASŁO



- Unikaj haseł powiązanych z informacjami o Tobie lub Twoich bliskich jak: imię, nazwisko, data lub miejsce urodzenia, imię pupila, powtórzenia frazy z loginu.

- Nie twórz haseł powtarzalnych, według schematów np.:
  mojehaslo1
  haslogrudzien2022

- Im dłuższe hasło, tym jest ono trudniejsze do złamania. Twórz hasła składające się z minimum 14 znaków. Dodaj znaki specjalne, cyfry lub zamień niektóre słowa na inne.

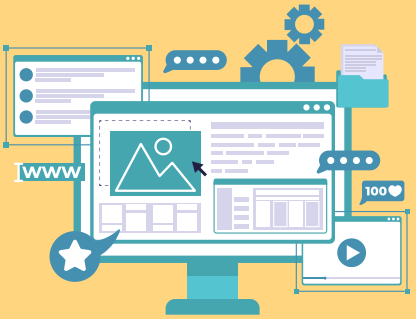
- Nie zapisuj haseł na karteczkach i nie przyklejaj ich na urządzeniu.

- Jedna usługa = jedno hasło. Do każdej usługi stwórz odrębne hasło.

- Ustaw weryfikację dwuetapową.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO



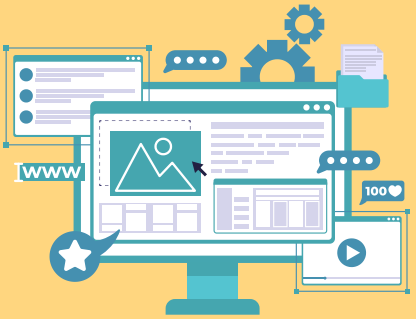
#USTAL Z BABCIĄ HASŁO

1 Opracowujcie w grupach 3 przykładowe hasła bezpieczeństwa, jakie moglibyście ustalić ze swoimi dziadkami. Podzielcie się swoimi pomysłami.

2 Opracujcie autorskie naklejki na telefon, tablet lub laptop, które w awaryjnych sytuacjach przypomną Waszym dziadkom żeby powstrzymali się od natychmiastowego działania, gdy otrzymają podejrzaną wiadomość e-mail lub odbiorą telefon będący potencjalną próbą ataku pishingowego.

3 Przekażcie swoje odgadnięte hasło krzyżówki online do Dyrektora Szkoły, którego zadaniem jest przesłanie zestawienia odgadniętych przez ¾ klas IV-VI funkcjonujących w Waszej Szkole haseł (kampanii) na adres: ustalhaslo@malopolska.uw.gov.pl, tak by Wasza Szkoła została umieszczona na mapie zwycięzców kampanii.

USTAL Z BABCIĄ HASŁO

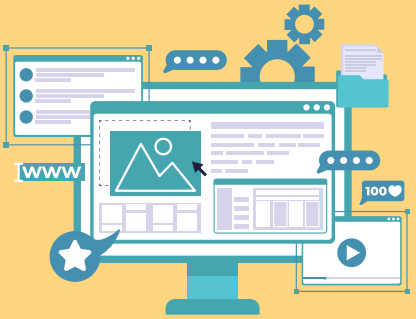


KRZYŻÓWKA NA ZAKOŃCZENIE LEKCJI, A ZARAZEM POTWIERDZENIE UDZIAŁU W KAMPANII:

https://learningapps.org/watch?v=prjet219326

#USTAL Z BABCIĄ HASŁO

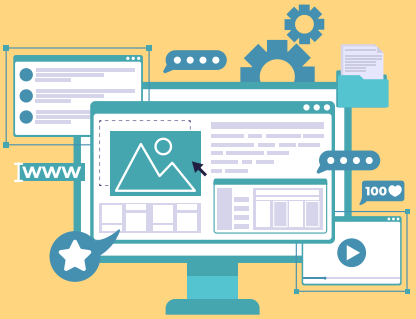
USTAL Z BABCIĄ HASŁO



#USTAL Z BABCIĄ HASŁO

Ustal hasło z Babcią i/ lub Dziadkiem, które będzie zawierało szczegół znany tylko Twojemu prawdziwemu członkowi rodziny.

USTAL Z BABCIĄ HASŁO



#USTAL Z BABCIĄ HASŁO

Zapraszamy także wszystkich uczniów do podjęcia się rozpromowania tej inicjatywy pod hasztagiem #UstalHasło. Każdy oryginalny i ciekawy filmik nakręcony z użyciem aplikacji TikTok, w którym zostanie umieszczony #UstalHasło, zostanie rozpowszechniony poprzez social media Małopolskiego Urzędu Wojewódzkiego w Krakowie oraz Kuratorium Oświaty w Krakowie, tak by Wasza sprawczość dotarła do jak największego grona osób zainteresowanych walką z oszustwami. Prześlijcie nam Wasze filmiki na adres: ustalhaslo@malopolska.uw.gov.pl