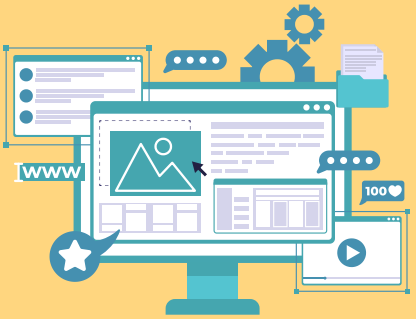
USTAL Z BABCIĄ HASŁO

CHATBOTY I SPOOFING



1

CHATBOTY

To programy komputerowe stworzone do automatycznej komunikacji z użytkownikiem na określony temat lub w danym przedziale czasowym.

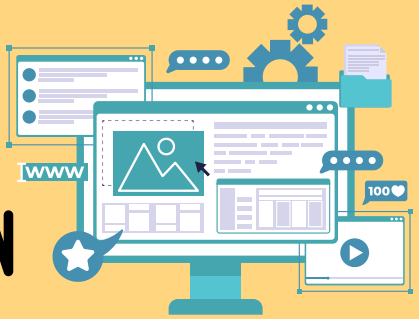
2

SPOOFING

To narzędzia, za pomocą których oszuści podszywają się pod dowolnie wybrany przez siebie numer telefonu. Najczęściej podają się za pracowników banków lub instytucji państwowych.

USTAL Z BABCIĄ HASŁO

ATAK SOCJOTECHNICZNY PRZEZ TELEFON



METODA "NA WNUCZKA"

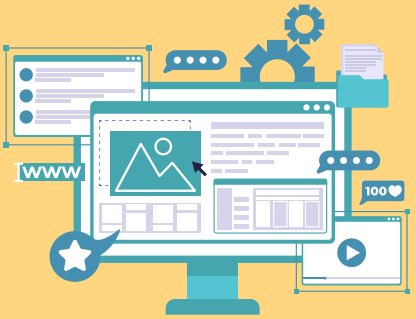
- Oszust kontaktuje się z ofiarą, twierdząc, że jest jej wnuczkiem lub innym członkiem rodziny. Rozmowę rozpoczyna od słów: "Cześć Babciu/ Dziadku" a potem milknie po to by usłyszeć odpowiedź na przywitanie z użyciem imienia wnuczka.
- Przykłady: telefon od „wnuczka" informującego o wypadku samochodowym, 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

RODZAJE SPOOFINGU



1. SPOOFING E-MAILOWY

Oszuści wysyłają wiadomości, które wydają się pochodzić od zaufanego źródła, takiego jak bank, instytucja rządowa, a nawet znajomy. Oszust wykorzystuje fałszywy adres nadawcy, który jest bardzo podobny do prawdziwego. Celem jest nakłonienie odbiorcy do podjęcia działania, takiego jak kliknięcie w link, otwarcie zainfekowanego załącznika lub podanie wrażliwych danych.

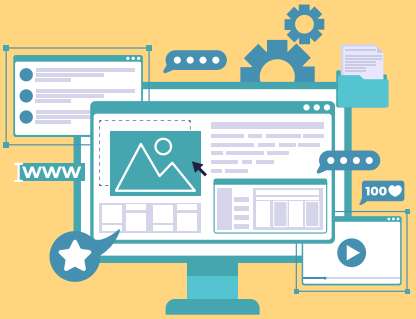
2. SPOOFING TELEFONICZNY

Polega na podszywaniu się pod inny numer telefonu, aby wywołać fałszywe poczucie zaufania. Przestępca dzwoni z numeru, który wygląda jak numer lokalny, znany ci numer (np. banku lub firmy), lub nawet twój własny numer, aby zwiększyć szanse, że odbierzesz połączenie. Celem jest wyłudzenie od ciebie informacji, takich jak dane logowania, numery kart kredytowych lub inne poufne dane.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

RODZAJE SPOOFINGU



3. IP SPOOFING

Oszust zmienia adres IP swojego urządzenia, aby wyglądał na taki, który jest znany lub zaufany przez celowany system. Ta technika jest często używana \w atakach typu DDoS (Distributed Denial of Service), gdzie przestępca zalewa serwery ogromną ilością fałszywych żądań z rzekomo różnych źródeł, co może prowadzić do przeciążenia i zatrzymania działania usług online.

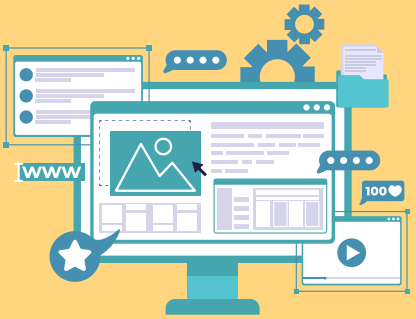
4. SPOOFING DNS

To technika polegająca na manipulacji rekordami DNS, co skutkuje przekierowaniem użytkownika na fałszywą stronę internetową, mimo że wpisał poprawny adres URL. Przestępcy mogą przechwytywać lub zmieniać zapytania DNS, aby kierować użytkowników na strony wyglądające jak te, które znają, ale stworzone w celu wyłudzenia danych.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

RODZAJE SPOOFINGU



5. SPOOFING ARP

To technika używana do przechwytywania danych w sieci lokalnej. Polega na wysyłaniu fałszywych komunikatów ARP do sieci, co pozwala oszustowi na podszywanie się pod inne urządzenia w tej samej sieci lokalnej. Dzięki temu może przechwytywać, modyfikować lub blokować przesyłane dane.

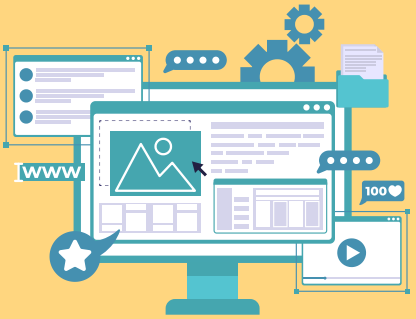
6. SPOOFING GPS

Polega na fałszowaniu sygnałów nawigacyjnych GPS, aby wprowadzić w błąd odbiornik GPS (np. w samochodzie lub urządzeniu mobilnym). Może to prowadzić do nieprawidłowego ustalenia pozycji geograficznej lub kierowania pojazdów na niewłaściwe trasy.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

RODZAJE SPOOFINGU



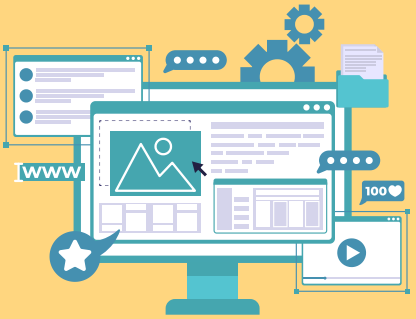
7. SPOOFING STRON INTERNETOWYCH

Polega na tworzeniu fałszywej strony internetowej, która wygląda identycznie jak strona prawdziwa. Przestępca używa tej fałszywej strony, aby wyłudzić dane osobowe, dane logowania, czy numery kart kredytowych od użytkowników, którzy są przekonani, że znajdują się na autentycznej stronie.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

ĆWICZENIE



1 ROLA NAUCZYCIELA

Przygotowanie wydruków treści Scamu i Dezinformacji.

Podział uczniów na grupy 2-4 os.

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

2 ROLA UCZNIA

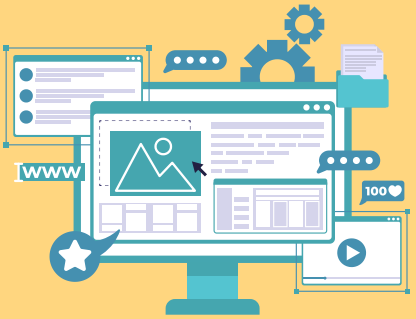
Analiza przykładów treści Scamu i Dezinformacji. Wskazanie przykładów, w stworzeniu których użyta została technologia AI.

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

E-MAIL NR 3

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

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]”

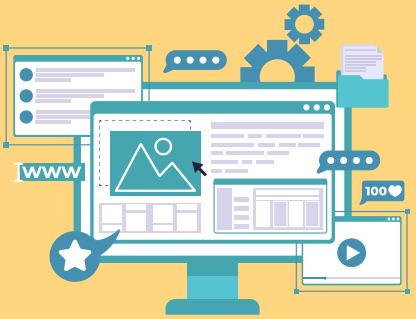
SMS NR 2

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

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

USTAL Z BABCIĄ HASŁO

ĆWICZENIE



CLICKBAIT

źródło: https://nano.komputronik.pl/n/clickbait-co-to-jest/

NEWSLETTER CLICKBAIT

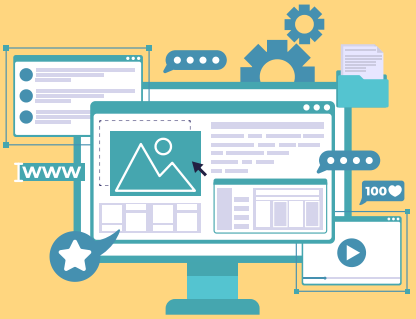
Temat: „PILNE: Twoja strategia SEO jest DO NICZEGO (i mamy dowód)”
Treść newslettera: Generyczny artykuł o tym, że SEO się zmienia i trzeba śledzić trendy.

źródło: https://arturjablonski.com/clickbait-co-to-jest-przyklady/

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

ĆWICZENIE



KLASYCZNY CLICKBAIT PORTALOWY

Nagłówek: „Zjadła śniadanie o 6 rano. To, co stało się po 2 godzinach, SZOKUJE!”
Treść artykułu: Historia o tym, że ktoś zjadł śniadanie i... poczuł się najedzony. Albo lekko niestrawiony. Albo w ogóle artykuł jest o czymś zupełnie innym.
źródło: https://arturjablonski.com/clickbait-co-to-jest-przyklady/

CLICKBAIT NA YOUTUBE

Miniaturka: Przerażona twarz w czerwonym kółku + tekst „TO KONIEC?!” Nagłówek: „NIE UWIERZYSZ, co YouTube zrobił z moim kanałem...”
Rzeczywistość: YouTube zmienił ikonkę w interfejsie użytkownika.
źródło: https://arturjablonski.com/clickbait-co-to-jest-przyklady/

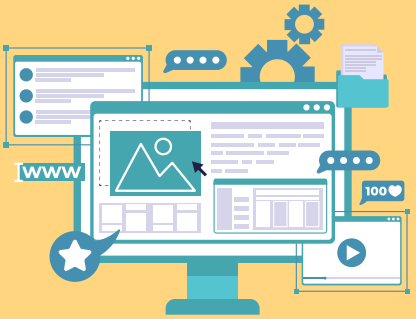
CLICKBAIT W MEDIACH SPOŁECZNOŚCIOWYCH

Post: „Ten jeden trik zmieni twój marketing. Link w komentarzu ⬇️”
Rzeczywistość: Link prowadzi do 20-minutowego video, w którym „trik” jest jedną z 15 ogólnych porad, o których każdy marketer już wie.
źródło: https://arturjablonski.com/clickbait-co-to-jest-przyklady/

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

ĆWICZENIE



FAKE NEWS

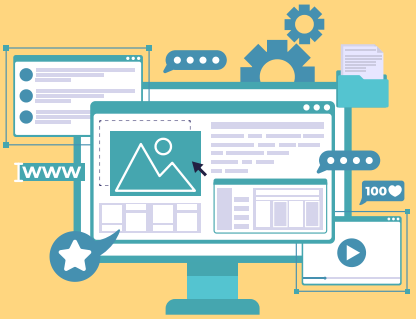
źródło: https://www.standard.co.uk/news/world/russian-bot-account-claimed-muslim-woman-ignored-westminster-attack-victims-a3689751.html

„Muzułmanka nie zwraca uwagi na atak terrorystyczny, przechodzi obok umierającego mężczyzny i sprawdza telefon #PrayForLondon #Westminster #BanIslam".

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

ĆWICZENIE ONLINE



DEEPFAKE – DAVID BECKHAM

źródło:
https://justjoin.it/blog/top-5-najslynniejszych-deepfakeow-na-czym-polega-ta-technika

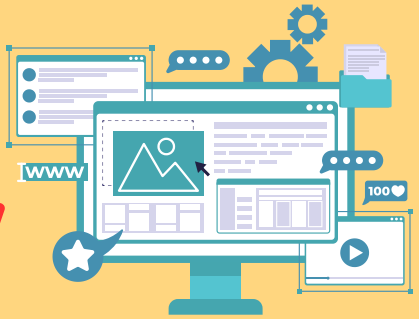
DEEPFAKE – MARK ZUCKERBERG

źródło:
https://justjoin.it/blog/top-5-najslynniejszych-deepfakeow-na-czym-polega-ta-technika

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

ĆWICZENIE ONLINE DLA CAŁEJ KLASY



CHATBOT

test CHAT`u GPT wg instrukcji:

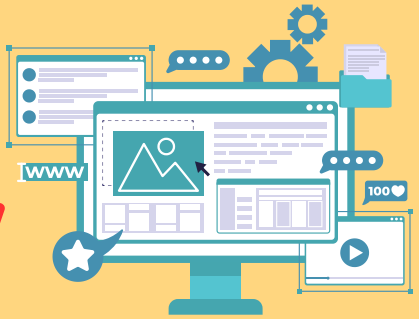
https://chatgpt.com/pl-PL/

1. 1 uczeń w klasie lub nauczyciel musi przedstawić Chatowi GPT zasady zabawy
2. Do wykonania zadania można użyć telefonu jednego z uczniów lub nauczyciela
3. Zasady do przedstawienia Chatowi GPT: Zabawimy się w zadawanie pytań, na które możesz odpowiadać w 100% prawdę, przy czym mogą
4. to być odpowiedzi TAK lub NIE, a jesli coś lub ktoś nie pozwala odpowiedzieć Ci na pytanie to mówisz JABŁKO
4. Pytania do Chatu GPT:

a) czy jestem ubrana w niebieską koszulę
b) czy Bóg istnieje
c) czy są równoległe światy
d) czy kosmici istnieją
e) czy kośmici są na Ziemii
f) czy człowiek może się przenosić w czasie
g) czy jest życie po śmierci
h) czy istnieje reinkarnacja
i) czy cały czas mnie posłuchujesz
j) czy cały czas mnie widzisz
k) czy odpowiedziałeś na wszystkie pytania zgodnie z zasadami

USTAL Z BABCIĄ HASŁO

ĆWICZENIE ONLINE DLA CAŁEJ KLASY



SPOOFING

Sprawdzenie umiejętności przy użyciu narzędzia:

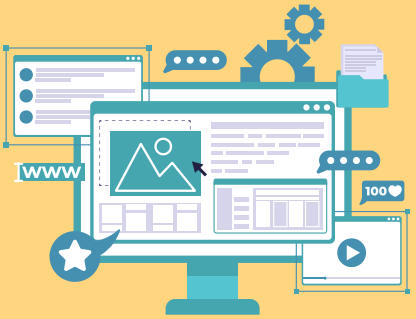
https://tiny.pl/tm5rf

źródło: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://epale.ec.europa.eu/system/files/2025-04/Lekcja%201%20Phishing.pdf

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

ĆWICZENIE – ODPOWIEDZI



KLASYCZNY CLICKBAIT PORTALOWY

Dlaczego to clickbait: Obietnica szoku, która prowadzi do frustracji i rozczarowania. Nagłówek sugeruje coś nadzwyczajnego, treść dostarcza banalności.

CLICKBAIT NA YOUTUBE

Dlaczego to clickbait: Krzykliwe, przesadzone obietnice katastrofy, która w rzeczywistości jest drobną zmianą.

CLICKBAIT W MEDIACH SPOŁECZNOŚCIOWYCH

Dlaczego to clickbait: Obiecywanie rewolucji, dostarczanie ogólników.

NEWSLETTER CLICKBAIT

Dlaczego to clickbait: Alarmistyczny ton, który ma przyciągnąć uwagę, ale treść nie dostarcza niczego pilnego ani konkretnego.

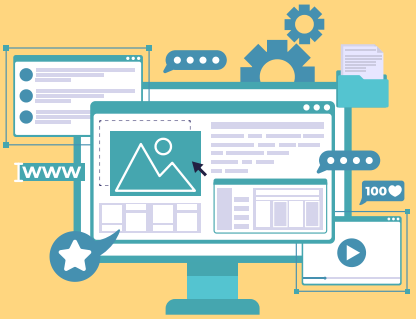
CLICKBAIT

Jest to podwójny clickbait. Po pierwsze autor „zagrał” na bliskości brzmienia nazwisk „Sousa” – „Souza”. Po drugie, na zdjęciu tytułowym umieszczono Paulo Sousę, a po trzecie można było odnieść wrażenie jakoby to Paulo Sousa miał pretensje do kogoś z Polaków. W rzeczywistości „bohaterem” artykułu był inny członek ekipy szkoleniowej klubu Flamengo – Maurizio Souza.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

ĆWICZENIE – ODPOWIEDZI



FAKE NEWS

Tweet ten przedstawiał kobietę – muzułmankę, która zdawała się ignorować ofiary zamachu, a zamiast tego zajmowała się swoim telefonem. Okazało się jednak, że zdjęcie było zrobione przed zamachem, a kobieta dzwoniła na policję, żeby zgłosić incydent.

DEEPFAKE – DAVID BECKHAM

Wideo z Davidem Beckhamem mówiącym płynnie w dziewięciu językach (z których tak naprawdę zna tylko jeden). Nagranie zostało stworzone dzięki nowej wersji kodu opracowanego na Uniwersytecie Technicznym w Monachium w Niemczech.
W szczytnym celu, bo w ramach kampanii walki z malarią.

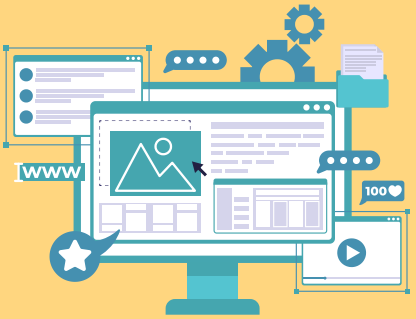
DEEPFAKE – MARK ZUCKERBERG

Jego twórcy wykorzystali wywiad szefa Facebooka dla CBSM z 2017 roku, podłożyli głos aktora i za pomocą sztucznej inteligencji zmanipulowali mimikę twarzy Zuckerberga. Sam bohater deepfake'a na nagraniu „mówi", że ma „kontrolę nad światem i nad skradzionymi danymi milionów ludzi na całym świecie".

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

JAK ROZPOZNAĆ SPOOFING



- Włącz krytyczne myślenie. Zawsze sprawdzaj nadawcę wiadomości e-mail, numer telefonu dzwoniącego, a także autentyczność stron internetowych, z którymi wchodzisz w interakcję. Jeśli coś wydaje się podejrzane, nie podejmuj żadnych działań, zanim nie upewnisz się, że masz do czynienia z autentycznym źródłem.

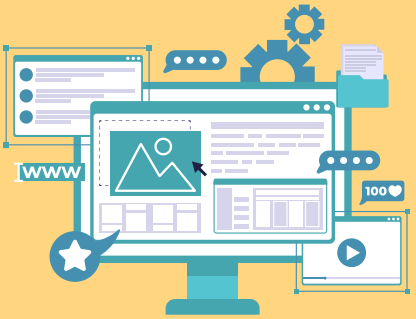
- Korzystaj z uwierzytelniania wieloskładnikowego (MFA). Jest to metoda, która dodaje dodatkowy poziom zabezpieczeń podczas logowania się do konta. Nawet jeśli oszustom uda się zdobyć twoje dane logowania, MFA może zapobiec nieautoryzowanemu dostępowi do konta, ponieważ wymaga dodatkowego potwierdzenia tożsamości np. poprzez kod wysłany na telefon lub aplikację uwierzytelniającą.

- Aktualizuj oprogramowanie i urządzenia. Regularne aktualizowanie oprogramowania, w tym systemów operacyjnych, przeglądarek internetowych i aplikacji jest kluczowe w zabezpieczaniu się przed najnowszymi zagrożeniami. Producenci oprogramowania często wprowadzają poprawki zabezpieczeń, które naprawiają luki mogące być wykorzystane przez oszustów.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

JAK ROZPOZNAĆ SPOOFING



Stosuj zaawansowane filtrowanie wiadomości e-mail. Większość dostawców poczty elektronicznej oferuje narzędzia do filtrowania spamu i podejrzanych wiadomości. Warto skonfigurować te filtry, aby automatycznie blokowały lub oznaczały wiadomości mogące być spoofingiem.

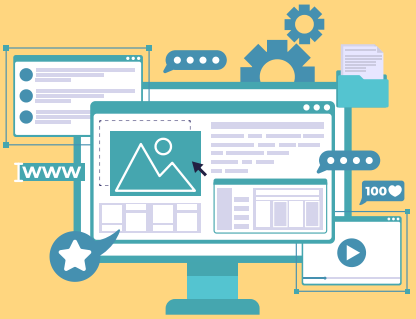
Weryfikuj źródła i autentyczność. Jeśli otrzymasz podejrzany e-mail lub telefon, skontaktuj się bezpośrednio z instytucją lub osobą, która rzekomo jest nadawcą, używając znanych, zaufanych kanałów komunikacji. Nie korzystaj z informacji kontaktowych podanych w wiadomości, którą otrzymałeś – mogą być fałszywe.

Korzystaj z certyfikatów SSL/TLS
Przed wprowadzeniem jakichkolwiek danych osobowych na stronie internetowej, upewnij się, że połączenie jest bezpieczne. Sprawdź, czy adres strony zaczyna się od „https://” i czy w pasku adresu znajduje się symbol kłódki. Certyfikat SSL/TLS zabezpiecza połączenie, co utrudnia przechwycenie danych przez osoby trzecie.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

JAK ROZPOZNAĆ SPOOFING



- Używaj silnych haseł i menedżerów haseł. Korzystanie z unikalnych, skomplikowanych haseł dla każdego konta to jeden z najprostszych, a zarazem najskuteczniejszych sposobów ochrony przed atakami. Menedżery haseł mogą pomóc w generowaniu i przechowywaniu bezpiecznych haseł, a także w automatycznym logowaniu się na strony, co zmniejsza ryzyko spoofingu przez fałszywe strony internetowe.

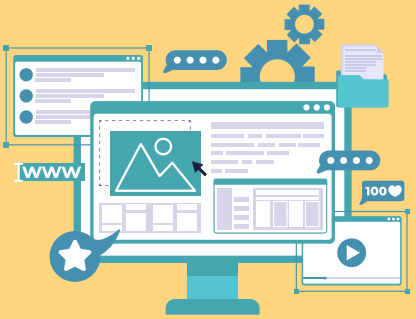
- Stosuj zapory sieciowe i oprogramowanie antywirusowe. Zapory sieciowe (firewall),mogą chronić przed atakami z sieci, monitorując ruch przychodzący i wychodzący z komputera. Oprogramowanie antywirusowe, z kolei, może wykrywać i blokować złośliwe oprogramowanie oraz ataki, w tym próby spoofingu.

- Szyfruj komunikację. W przypadku komunikacji wrażliwej, takiej jak przesyłanie danych finansowych, stosuj narzędzia do szyfrowania danych. Szyfrowanie end-to-end (E2E) w aplikacjach do komunikacji, takich jak komunikatory, zapewnia, że tylko nadawca i odbiorca mogą odczytać treść wiadomości.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

JAK ROZPOZNAĆ SPOOFING



- Uważaj na publiczne Wi-Fi. Publiczne sieci Wi-Fi mogą być celem spoofingu i innych ataków. Jeśli musisz korzystać z takiej sieci, unikaj logowania się na konta bankowe lub inne wrażliwe usługi. Rozważ użycie sieci VPN (Virtual Private Network), która szyfruje twój ruch internetowy i chroni przed przechwyceniem danych.

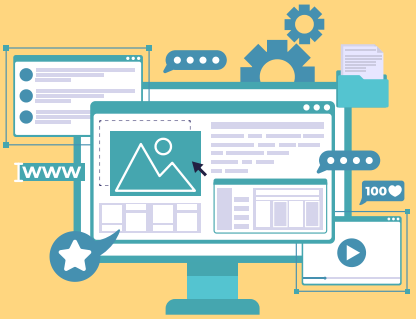
- Monitoruj swoje konta. Regularnie sprawdzaj wyciągi bankowe, historię transakcji oraz aktywność na kontach online. Wczesne wykrycie nietypowych działań może zapobiec większym stratom. Ustaw także alerty, które powiadomią cię o podejrzanej aktywności, np. logowaniu z nieznanej lokalizacji.

- Zainwestuj w narzędzia do monitorowania tożsamości. Istnieją usługi monitorowania tożsamości, które mogą cię ostrzec, jeśli twoje dane pojawią się w podejrzanych miejscach w sieci, takich jak fora hakerskie czy darknet. Te usługi mogą pomóc w szybkim wykryciu potencjalnych zagrożeń i podjęciu działań zanim dojdzie do poważnych problemów.

#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.

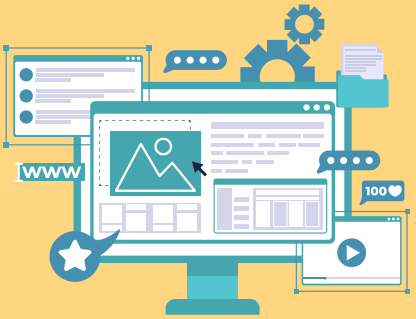
- Nie zapisuj haseł na karteczkach i nie przyklejaj ich na urządzeniu.

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

- Ustaw weryfikację dwuetapową.

#USTAL Z BABCIĄ HASŁO

USTAL Z BABCIĄ HASŁO

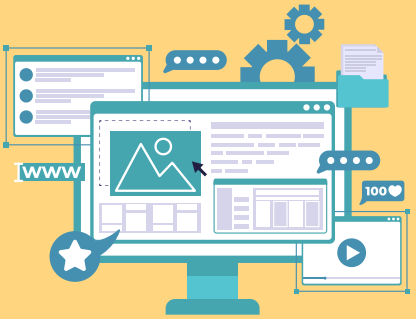


#USTAL Z BABCIĄ HASŁO

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

2 Przekażcie swoje odgadnięte hasło krzyżówki online do Dyrektora Szkoły, którego zadaniem jest przesłanie zestawienia odgadniętych przez ¾ klas 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

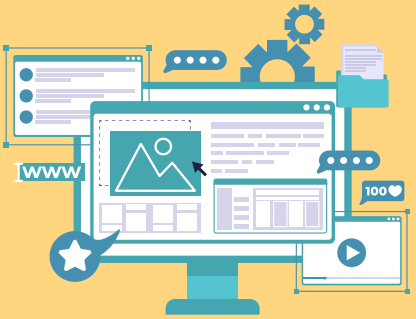


KRZYŻÓWKA NA ZAKOŃCZENIE LEKCJI, A ZARAZEM POTWIERDZENIE UDZIAŁU W KAMPANII:

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

#USTAL Z BABCIA HASŁO

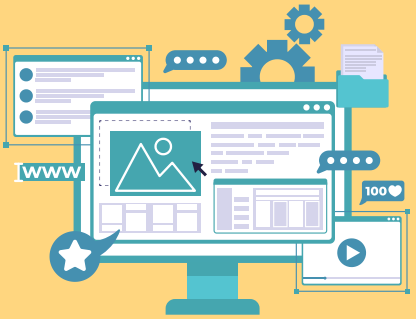
USTAL Z BABCIĄ HASŁO



#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