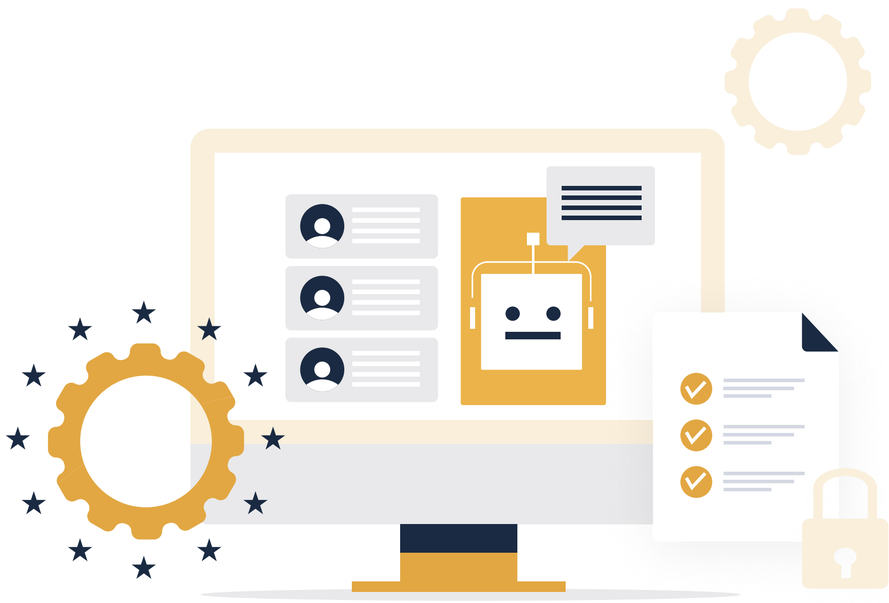
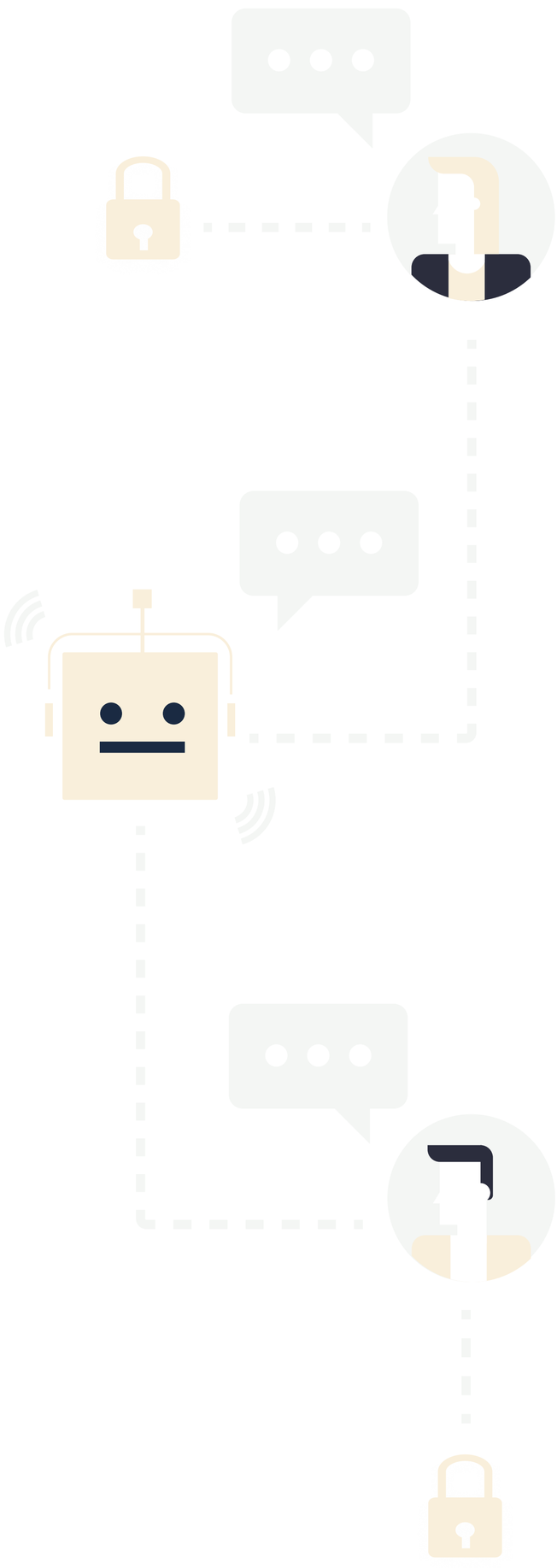
VII Rocznica obowiązywania RODO

25 maja 2025r.

Jak bezpiecznie korzystać z narzędzi AI?

Generatywna AI (czyli np. Open AI, Vertex AI, ChatGPT lub Microsoft Copilot) zbiera i przechowuje różnego rodzaju dane za pomocą swoich platform. Dlatego musisz upewnić się, że korzystając ze sztucznej inteligencji, nie przekazujesz wrażliwych danych o sobie, swojej firmie czy rodzinie.





Podstawowe zasady korzystania z AI

- Narzędzia oparte na AI powinny być używane w organizacji wyłącznie w celach związanych z wykonywanymi działaniami, celami i za zgodą osób decyzyjnych
- Osoby odpowiedzialne za ochronę danych osobowych w organizacji powinny ocenić dane narzędzie AI, biorąc pod uwagę m.in kwestię prywatności
- Organizacja nie powinna korzystać z narzędzi AI w sposób dyskryminujący lub mogący powodować skutki dla osób fizycznych czy prawnych
  Użycie narzędzi AI musi być zgodne ze wszystkimi obowiązującymi przepisami prawa i regulacjami
- Jeśli materiał wytworzony przez AI będzie udostępniany, organizacja powinna podjąć działania, aby dokonać przeglądu treści pod kątem plagiatu przed upowszechnieniem treści
- Korzystanie z narzędzia AI przez organizację zawsze powinno być poprzedzone zawarciem umowy, w tym w uzasadnionych przypadkach również umowy powierzającej dane osobowe w przetwarzanie
- Organizacja powinna podejmować działania, aby zobowiązać zewnętrznych dostawców świadczących usługi do informowania o użyciu AI w celu realizacji danej usługi
- Przed użyciem AI, które będzie wiązać się z wykorzystaniem danych osobowych, należy przeprowadzić ocenę ryzyka wpływu tego przetwarzania na osoby fizyczne, w tym również bezwzględnie ocenę skutków dla ochrony danych
- Organizacja musi dbać o powiadomienie osób nadzorujących prawo do prywatności o planowaniu wykorzystania narzędzi AI w danym procesie

VII Rocznica obowiązywania RODO

25 maja 2025r.

Na co zwrócić uwagę, korzystając z AI

Wynik powinien być punktem wyjścia do dalszej pracy, wymagającej zaangażowania i wiedzy człowieka. Organizacja powinna wykluczyć lub ograniczyć (w uzasadnionych przypadkach) używanie wyniku bez przetworzenia go przez człowieka na produkt końcowy.

Treści generowane przez AI w uzasadnionych przypadkach wymagają przeglądu i akceptacji osób odpowiedzialnych za ponoszone ryzyko korporacyjne.

Organizacja powinna pamiętać, że ponosi odpowiedzialność za wszelkie szkody wyrządzone przez treści generowane przez AI w jej mieniu i na jej rzecz.

Organizacja powinna podjąć kroki, aby upewnić się, że dostawca usługi lub produktu zapewnia licencję umożliwiającą korzystanie z tych produktów zgodnie z zamierzonym celem.

Organizacja (jeśli to możliwe) powinna zakazać wprowadzania danych wrażliwych i poufnych do narzędzi AI, ponieważ nie są one przystosowane do ich bezpiecznego przetwarzania.

Zakazane praktyki AI

Stosowanie technik podprogowych, manipulacyjnych lub wprowadzających w błąd

Wykorzystywanie słabości osoby fizycznej lub grupy osób ze względu na ich wiek, niepełnosprawność lub szczególną sytuację społeczną lub ekonomiczną

Scoring społeczny

Profilowanie osoby fizycznej lub ocena jej cech osobowości, którego celem jest ocena ryzyka popełnienia przestępstwa

Stosowanie systemów rozpoznawania twarzy w czasie rzeczywistym poprzez nieukierunkowane pobieranie obrazów twarzy z Internetu lub nagrań CCTV

Wyciąganie wniosków na temat emocji osoby fizycznej w miejscu pracy lub instytucjach edukacyjnych.

Wykorzystywanie systemów kategoryzacji biometrycznej wnioskującychna temat rasy, poglądów politycznych, przynależności do związków zawodowych, przekonań religijnych lub światopoglądowych, seksualności lub orientacji seksualnej

Wykorzystywanie systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw

VII Rocznica obowiązywania RODO

25 maja 2025r.

Nowe rodzaje ataków hakerskich z przykładami. Jak się obronić?

AI-phishing / Deepfake czyli **Wiadomości i rozmowy generowane przez AI, często z voice cloningiem** na przykład **Fałszywy telefon od „dyrektora" z prośbą o przelew**

Przykład rzeczywistego incydentu:

W jednym z przypadków firma z Hongkongu straciła ponad 25 milionów dolarów w wyniku ataku typu deepfake. Oszuści wykorzystali sztuczną inteligencję do stworzenia realistycznych wideo i audio, które imitowały głos oraz wygląd dyrektora finansowego firmy. Pracownicy zostali zmanipulowani do wykonania serii przelewów, które okazały się oszustwem.

Zalecenia w celu ochrony przed tego typu atakami:

Szkolenia

Edukuj kadrę w zakresie rozpoznawania deepfake'ów i innych zaawansowanych technik oszustw

Wdrażanie procedur weryfikacji tożsamości

takich jak potwierdzanie przelewów za pomocą dwóch niezależnych kanałów komunikacji

Używanie narzędzi do analizy wideo i audio

które mogą pomóc w wykrywaniu manipulacji

Ostrożność w przypadku niespodziewanych lub pilnych próśb o przelewy

nawet jeśli pochodzą od znanych osób

VII Rocznica obowiązywania RODO

25 maja 2025r.

Quishing (QR-phishing) czyli **Złośliwe kody QR prowadzące do fałszywych stron** na przykład **Naklejka z kodem QR w restauracji przekierowuje do fałszywej płatności**

Przykład rzeczywistego incydentu:

Atak na użytkowników ING Banku w Holandii

W Holandii oszuści wykorzystali funkcję generowania kodów QR w aplikacji mobilnej ING Banku. Podszywali się pod kupujących na platformach sprzedażowych, prosząc o numer konta - rzekomo w celu dokonania płatności. Następnie wysyłali ofierze kod QR, który po zeskanowaniu dodawał ich urządzenie jako zaufane do konta bankowego ofiary, umożliwiając przechwycenie środków.

Atak na użytkowników aplikacji Signal przez rosyjskie grupy wywiadowcze

W lutym 2025 roku rosyjskie grupy wywiadowcze UNC5792 i UNC4221 wykorzystały technikę phishingową z kodami QR w aplikacji Signal, aby przejąć prywatne wiadomości użytkowników, szczególnie w Ukrainie. Wysyłali oni wiadomości z kodami QR, które po zeskanowaniu przez ofiarę umożliwiały zdalne połączenie urządzenia z kontem atakującego, dając pełny dostęp do komunikacji. Signal zareagował aktualizacjami, wprowadzając dodatkowe mechanizmy weryfikacji tożsamości, aby zapobiec takim atakom.

Zalecenia w celu ochrony przed tego typu atakami:

Ostrożność przy kodach QR z nieznanych źródeł

unikaj skanowania kodów z e-maili, SMS-ów czy plakatów bez weryfikacji ich autentyczności

Sprawdzanie adresów URL

po zeskanowaniu kodu upewnij się, że adres strony zaczyna się od "https://" i pochodzi z zaufanej domeny

Używanie aplikacji antywirusowych

niektóre aplikacje oferują funkcje skanowania kodów QR pod kątem bezpieczeństwa

Ostrożność z danymi osobowymi

nie podawaj swoich danych logowania, numerów kart kredytowych czy innych wrażliwych informacji na stronach, które zostały otwarte za pomocą kodu QR

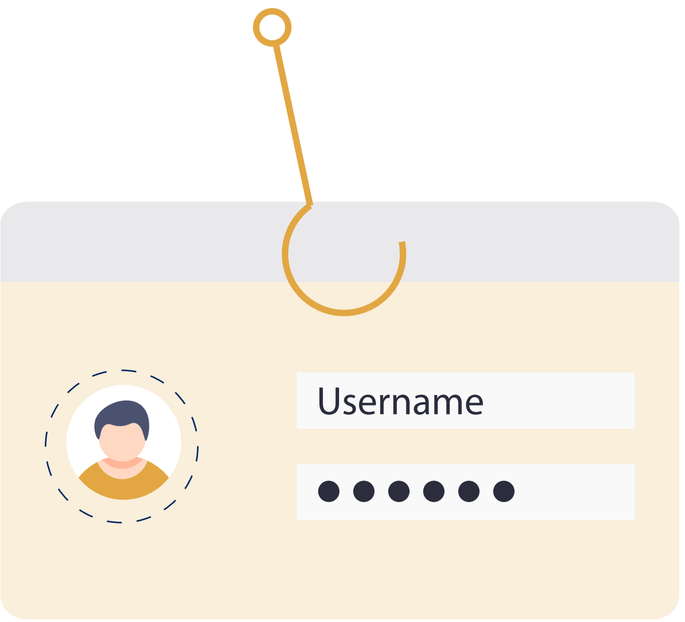
VII Rocznica obowiązywania RODO

25 maja 2025r.

Smishing / Vishing 2.0 czyli **SMS-y i połączenia z AI podszywające się pod znane instytucje** na przykład **SMS od „InPost” z linkiem do śledzenia paczki – fałszywy**

Przykład rzeczywistego incydentu:

W lutym 2025 roku w Polsce odnotowano wzrost liczby ataków typu smishing i vishing, w których oszuści podszywają się pod pracowników banków, firm kurierskich oraz instytucji państwowych. Ofiary otrzymują SMS-y lub e-maile z prośbą o kliknięcie w link lub zadzwonienie na numer telefonu, który prowadzi do fałszywej strony logowania lub infolinii. W jednym z przypadków, osoba otrzymała SMS z informacją o rzekomej próbie logowania do jej konta bankowego i prośbą o potwierdzenie tożsamości. Po kliknięciu w link, użytkownik został przekierowany na stronę imitującą stronę banku i podał swoje dane logowania, co skutkowało utratą środków z konta.



Zalecenia w celu ochrony przed tego typu atakami:

Weryfikacja źródła komunikacji

Nigdy nie klikaj w linki ani nie odbieraj połączeń od nieznanych numerów. Jeśli otrzymasz wiadomość od rzekomej instytucji, skontaktuj się z nią bezpośrednio, korzystając z oficjalnych danych kontaktowych

Zabezpieczenie konta bankowego

Używaj silnych haseł i włącz dwuskładnikowe uwierzytelnianie (2FA) wszędzie tam, gdzie to możliwe

Edukacja i świadomość

Regularnie uczestnicz w szkoleniach z zakresu bezpieczeństwa cyfrowego i bądź świadomy najnowszych zagrożeń

Zgłaszanie incydentów

Jeśli padniesz ofiarą takiego ataku, niezwłocznie zgłoś to swojemu bankowi oraz odpowiednim służbom ścigania lub na CERT.pl

VII Rocznica obowiązywania RODO

25 maja 2025r.

SaaS phishing czyli **Podszywanie się pod usługi chmurowe** na przykład **Fałszywe zaproszenie do Google Docs prowadzące do strony logowania**

Przykład rzeczywistego incydentu:

W maju 2025 roku eksperci ds. bezpieczeństwa ostrzegli przed zaawansowanym atakiem phishingowym skierowanym do użytkowników Gmaila. Atak polegał na wysyłaniu e-maili podszywających się pod oficjalne powiadomienia od organów ścigania. W wiadomości znajdował się link prowadzący do fałszywej strony logowania, hostowanej na subdomenie Google Sites, gdzie ofiary były proszone o podanie swoich danych logowania. Dzięki wykorzystaniu subdomeny google.com, strona wyglądała na autentyczną, co zwiększało skuteczność ataku.

Zalecenia w celu ochrony przed tego typu atakami:

Weryfikacja źródła

zawsze sprawdzaj adres URL strony, na którą jesteś przekierowywany. Upewnij się, że pochodzi z oficjalnej domeny i nie zawiera podejrzanych subdomen

Używanie menedżerów haseł

korzystaj z menedżerów haseł, które automatycznie wypełniają dane logowania tylko na zaufanych stronach

Szkolenie pracowników

regularnie przeprowadzaj szkolenia z zakresu rozpoznawania prób phishingu i bezpiecznego korzystania z aplikacji SaaS

Wdrażanie uwierzytelniania wieloskładnikowego (MFA)

MFA znacząco utrudnia przejęcie konta, nawet jeśli dane logowania zostaną skradzione

Monitorowanie aktywności

regularnie sprawdzaj logi aktywności w aplikacjach SaaS pod kątem podejrzanych działań, takich jak nieautoryzowane logowania czy zmiany ustawień

VII Rocznica obowiązywania RODO

25 maja 2025r.

Browser-in-the-browser czyli **Fałszywe okna logowania wygenerowane w przeglądarce** na przykład **Okno „Log in with Google" to tak naprawdę element HTML**

Przykład rzeczywistego incydentu:

Atak na użytkowników portalu bankowego

W jednym z przypadków oszuści wysyłali e-maile, które wyglądały na powiadomienia od banków. W e-mailu znajdował się link, który prowadził do strony z fałszywym oknem logowania. Po kliknięciu na link otwierało się nowe okno w przeglądarce, które wyglądało jak oryginalna strona logowania do banku. Jednak w rzeczywistości była to tylko strona stworzona przez oszustów. Ponieważ okno było wyświetlane w obrębie tej samej przeglądarki, użytkownicy nie zauważali żadnej nieprawidłowości.

Atak na usługi Google

Oszuści rozsyłali e-maile przypominające powiadomienia o próbie logowania do konta Google. Link w wiadomości prowadził do fałszywej strony, która imitowała prawdziwą stronę logowania Google, ale była to tylko zmanipulowana strona, wyświetlana w formie okna przeglądarki. Wprowadzone przez ofiarę dane logowania były natychmiast przechwytywane przez oszustów.

Zalecenia w celu ochrony przed tego typu atakami:

Weryfikacja adresu URL

zawsze sprawdzaj, czy adres URL w pasku przeglądarki jest autentyczny, a strona zaczyna się od https://. Jeśli logujesz się do banków, mediów społecznościowych lub usług, wpisuj adres ręcznie, zamiast klikać w linki w wiadomościach e-mail

Używanie menedżerów haseł

menedżer haseł może automatycznie wypełniać dane logowania tylko na zaufanych stronach, co zmniejsza ryzyko oszustwa

Dwuskładnikowe uwierzytelnianie (2FA)

zawsze włączaj dwuskładnikowe uwierzytelnianie na swoich kontach, aby dodać dodatkową warstwę ochrony, nawet jeśli dane logowania zostaną skradzione

Ostrożność przy e-mailach

nigdy nie klikaj na podejrzane linki w e-mailach. Jeśli otrzymasz powiadomienie o próbie logowania, zaloguj się bezpośrednio na stronie przez wpisanie adresu ręcznie, zamiast kliknąć w link

Aktualizacje oprogramowania

regularnie aktualizuj przeglądarki internetowe oraz aplikacje zabezpieczające przed phishingiem, które mogą wykrywać podejrzane strony

VII Rocznica obowiązywania RODO

25 maja 2025r.

Spear phishing 2.0 czyli **Spersonalizowane e-maile lub wiadomości na bazie OSID/OSIDNT** na przykład **Wiadomość od „działu IT” z nazwiskiem Twojego kolegi**

Spear phishing 2.0 to nowoczesna i bardziej wyrafinowana wersja tradycyjnego ataku phishingowego, w której cyberprzestępcy wykorzystują **personalizowane** techniki do wyłudzania poufnych informacji, takich jak dane logowania, numery kart kredytowych, czy dane firmowe. W wersji 2.0, atakujący wykorzystują **szeroką gamę nowoczesnych narzędzi i dane z mediów społecznościowych** oraz **informacje dostępne publicznie**, aby stworzyć bardziej wiarygodne i trudniejsze do wykrycia ataki.

Przykład rzeczywistego incydentu:

Atak na firmę finansową

W marcu 2025 roku firma finansowa w USA padła ofiarą ataku Spear Phishing 2.0. Hakerzy przeanalizowali publiczne profile pracowników na LinkedIn i zbierali informacje o ich roli w firmie oraz bieżących projektach. Jedna z wiadomości e-mail, która wydawała się pochodzić od dyrektora firmy, zawierała prośbę o zatwierdzenie faktury za usługi zewnętrznej firmy. Wiadomość była bardzo szczegółowa, odnosiła się do projektu, nad którym pracował odbiorca. Po kliknięciu w link, ofiara została przekierowana na stronę logowania do systemu bankowego, skąd dane logowania zostały przechwycone przez cyberprzestępców.

Zalecenia w celu ochrony przed tego typu atakami:

Weryfikacja nadawcy

zawsze upewnij się, że wiadomość pochodzi z oficjalnego adresu e-mail. W przypadku jakichkolwiek wątpliwości, skontaktuj się z nadawcą za pośrednictwem znanych kanałów

Uwierzytelnianie dwuskładnikowe (2FA)

Włącz dwuskładnikowe uwierzytelnianie na wszystkich kontach, które obsługują tę funkcję. Nawet jeśli dane logowania zostaną skradzione, 2FA będzie stanowiło dodatkową warstwę ochrony

Edukacja pracowników

regularnie szkól swoich pracowników z zakresu rozpoznawania prób phishingowych i oszustw. Ważne jest, aby byli oni świadomi technik wykorzystywanych przez cyberprzestępców, zwłaszcza tych bardziej zaawansowanych

Używanie menedżerów haseł

menedżer haseł automatycznie wypełnia formularze logowania na zaufanych stronach, co pomaga zapobiegać oszustwom związanym z fałszywymi stronami logowania

Ochrona przed złośliwym oprogramowaniem

zainstaluj oprogramowanie antywirusowe i regularnie skanuj systemy pod kątem zagrożeń. Większość nowoczesnych programów antywirusowych oferuje również ochronę przed phishingiem

Zgłaszanie podejrzanych działań

Jeżeli masz jakiekolwiek podejrzenia co do autentyczności otrzymanej wiadomości, niezwłocznie zgłoś to odpowiednim służbom bezpieczeństwa lub zespołowi IT w firmie

VII Rocznica obowiązywania RODO

25 maja 2025r.

SEO phishing / Ad phishing czyli **Fałszywe strony w Google i reklamach** na przykład **Reklama np. banku prowadzi do identycznie wyglądającej strony phishingowej**

Przykład rzeczywistego incydentu:

Reklama o "**wygłoszeniu nagrody**": Przestępcy uruchomili kampanię reklamową w Google Ads, która wyświetlała użytkownikom reklamę mówiącą, że "wygrali nagrodę". Po kliknięciu w reklamę użytkownicy byli przekierowywani na stronę, która wyglądała jak znana strona banku. Na tej stronie ofiary były proszone o zalogowanie się, a wprowadzone dane zostały przejęte przez przestępców.

Zalecenia w celu ochrony przed tego typu atakami:

Używanie sprawdzonych źródeł

zamiast klikać w linki z wyników wyszukiwania, wpisuj adresy stron ręcznie lub korzystaj z bezpośrednich linków, które masz zapisane lub które otrzymujesz od wiarygodnych źródeł

Instalacja oprogramowania zabezpieczającego

używaj oprogramowania antywirusowego i narzędzi do blokowania reklam, które mogą pomóc w wykrywaniu i blokowaniu złośliwych reklam i stron phishingowych

Sprawdzanie adresów URL

zawsze sprawdzaj, czy adres URL w pasku przeglądarki jest poprawny i zaczyna się od "https://". Phishingowe strony mogą mieć bardzo podobne adresy do oryginalnych, ale z drobnymi różnicami

Brak interakcji z podejrzanymi reklamami

jeśli reklama obiecuje coś zbyt dobrego, np. za darmo jakieś usługi, pieniądze, czy prezenty, bądź ostrożny. To może być klasyczny przypadek phishingu

Korzystanie z menedżera haseł

Menedżer haseł automatycznie wypełnia formularze logowania tylko na stronach, które są wiarygodne. Dzięki temu zmniejszasz ryzyko wprowadzenia danych na fałszywej stronie