BEZPIECZEŃSTWO W CYFROWYM ŚWIECIE.
Praktyczne zasady ochrony danych, kont i urządzeń

Technologie cyfrowe są dziś integralną częścią funkcjonowania organizacji, instytucji publicznych, przedsiębiorstw oraz naszego życia prywatnego. Ułatwiają komunikację, zarządzanie dokumentacją, korzystanie z usług publicznych, wykonywanie płatności, pracę zespołową czy realizację wielu codziennych obowiązków.

Wraz z rozwojem technologii pojawiają się jednak również nowe zagrożenia. Phishing, przejmowanie kont, wyłudzanie danych, kradzież tożsamości, złośliwe oprogramowanie, dezinformacja czy ataki socjotechniczne mogą dotknąć zarówno duże instytucje, jak i niewielkie organizacje oraz indywidualnych użytkowników.

Cyberbezpieczeństwo nie powinno być traktowane wyłącznie jako zagadnienie techniczne. To również **codzienne nawyki, odpowiedzialne zarządzanie informacją, świadomość zagrożeń oraz umiejętność właściwego reagowania na incydenty**.

Poniższa lista kontrolna zawiera podstawowe działania, które mogą pomóc zwiększyć bezpieczeństwo cyfrowe użytkownika i organizacji. Nie wszystkie rozwiązania trzeba

Centrum Obywatelskie Centrum C 10
os. Centrum C 10, 31-931 Kraków
e-mail: c10@ipp.expert
tel./SMS: 578 562 000

wdrożyć jednocześnie. Najważniejsze jest systematyczne podnoszenie poziomu bezpieczeństwa i regularne aktualizowanie stosowanych zabezpieczeń.

ZADBAJ O SILNE I UNIKALNE HASŁA

1. Ustaw silne hasło do komputera

Hasło chroniące komputer powinno być odpowiednio długie i trudne do odgadnięcia. Należy unikać prostych haseł, popularnych słów, dat urodzenia, imion czy łatwych do przewidzenia kombinacji znaków. Dobrym rozwiązaniem może być długa, łatwa do zapamiętania fraza, która jednocześnie będzie trudna do odgadnięcia przez inne osoby.

2. Korzystaj z menedżera haseł

Menedżer haseł umożliwia bezpieczne przechowywanie danych logowania oraz generowanie unikalnych haseł do poszczególnych usług. Dzięki temu nie trzeba używać jednego hasła w wielu serwisach ani samodzielnie zapamiętywać wszystkich danych logowania.

3. Zabezpiecz menedżer haseł

Do menedżera haseł należy ustawić silne i unikalne hasło główne. Jeżeli aplikacja oferuje dodatkowe zabezpieczenia, np. uwierzytelnianie wieloskładnikowe lub logowanie biometryczne – warto z nich korzystać.

4. Zainstaluj menedżer haseł na wykorzystywanych urządzeniach

Jeżeli wybrane rozwiązanie na to pozwala, warto korzystać z menedżera haseł na komputerze i urządzeniach mobilnych. Ułatwia to stosowanie silnych, unikalnych haseł w codziennej pracy.

5. Korzystaj z integracji menedżera haseł z przeglądarką

Oficjalne rozszerzenie wybranego menedżera haseł może ułatwić bezpieczne uzupełnianie danych logowania i ograniczyć potrzebę ręcznego wpisywania haseł.

Centrum Obywatelskie Centrum C 10
os. Centrum C 10, 31-931 Kraków
e-mail: c10@ipp.expert
tel./SMS: 578 562 000

6. Nie używaj tego samego hasła w wielu serwisach

Jeżeli jedno hasło zostało wykorzystane w kilku miejscach, jego ujawnienie może zagrozić wszystkim kontom zabezpieczonym w ten sam sposób. Każde ważne konto powinno posiadać własne, unikalne hasło.

WŁĄCZ DODATKOWE ZABEZPIECZENIA KONT

1. Włącz uwierzytelnianie wieloskładnikowe

Tam, gdzie jest to możliwe, należy aktywować uwierzytelnianie dwu- lub wieloskładnikowe (2FA/MFA). Oznacza to, że samo poznanie hasła nie wystarczy do zalogowania się na konto – konieczne będzie dodatkowe potwierdzenie tożsamości. W zależności od usługi można korzystać m.in. z aplikacji uwierzytelniających, kluczy sprzętowych lub innych dostępnych metod.

ZACHOWAJ OSTROŻNOŚĆ WOBEC PHISHINGU I PRÓB OSZUSTWA

1. Sprawdzaj adres strony internetowej przed podaniem danych

Przed wpisaniem loginu, hasła, danych osobowych lub informacji dotyczących płatności sprawdź, czy znajdujesz się na właściwej stronie internetowej. Oszuści często tworzą witryny bardzo podobne do stron banków, sklepów internetowych, firm kurierskich, serwisów aukcyjnych czy instytucji publicznych.

2. Zachowaj ostrożność podczas korzystania z kodów QR

Kod QR może prowadzić zarówno do bezpiecznej, jak i fałszywej strony internetowej. Przed podaniem danych po zeskanowaniu kodu należy zweryfikować adres strony, na którą nastąpiło przekierowanie. Szczególną ostrożność warto zachować wobec kodów QR pochodzących z nieznanego lub niezweryfikowanego źródła.

3. Uważaj na skrócone linki

Skrócone adresy internetowe mogą utrudniać ocenę, do jakiej strony rzeczywiście prowadzi odnośnik. Nie oznacza to, że każdy skrócony link jest niebezpieczny, ale

Centrum Obywatelskie Centrum C 10
os. Centrum C 10, 31-931 Kraków
e-mail: c10@ipp.expert
tel./SMS: 578 562 000

przed jego otwarciem – szczególnie w wiadomości pochodzącej z nieznanego źródła – warto zachować dodatkową ostrożność.

4. Korzystaj z zapisanych zakładek do ważnych serwisów

Strony banków, poczty elektronicznej czy innych często wykorzystywanych usług można zapisać w zakładkach przeglądarki. Pozwala to ograniczyć ryzyko przypadkowego wejścia na fałszywą stronę poprzez link przesłany w wiadomości lub znaleziony w wynikach wyszukiwania.

5. Weryfikuj tożsamość rozmówcy

Jeżeli ktoś prosi o przekazanie danych, wykonanie przelewu, podanie kodu, zmianę danych logowania lub podjęcie innej nietypowej czynności, warto zweryfikować jego tożsamość innym kanałem. Oszuści mogą podszywać się m.in. pod banki, firmy kurierskie, pracowników instytucji, przełożonych, współpracowników, znajomych czy członków rodziny. W razie wątpliwości skontaktuj się bezpośrednio z daną osobą lub instytucją, korzystając ze znanych i oficjalnych danych kontaktowych.

SPRAWDZAJ, CZY TWOJE DANE NIE ZOSTAŁY UJAWNIONE

1. Monitoruj informacje o wyciekach danych

Warto okresowo sprawdzać, czy adres e-mail lub inne dane związane z użytkowanymi kontami nie pojawiły się w znanych wyciekach danych. Można korzystać w tym celu z wiarygodnych serwisów informujących o naruszeniach bezpieczeństwa. Jeżeli otrzymasz informację o wycieku danych, sprawdź, jakich informacji dotyczył incydent, zmień zagrożone dane logowania i zweryfikuj zabezpieczenia pozostałych kont.

CHROŃ SWOJE URZĄDZENIA I PRZECHOWYWANE DANE

1. Włącz szyfrowanie dysku

Szyfrowanie dysku ogranicza możliwość uzyskania dostępu do zapisanych danych w przypadku utraty lub kradzieży urządzenia. Systemy operacyjne oferują wbudowane

Centrum Obywatelskie Centrum C 10
os. Centrum C 10, 31-931 Kraków
e-mail: c10@ipp.expert
tel./SMS: 578 562 000

rozwiązania umożliwiające szyfrowanie danych, np. BitLocker w systemie Windows czy FileVault w macOS.

2. Aktualizuj system i oprogramowanie

Regularnie instaluj aktualizacje systemu operacyjnego, przeglądarki internetowej, aplikacji oraz pozostałego oprogramowania. Aktualizacje często zawierają poprawki usuwające wykryte podatności bezpieczeństwa.

3. Zabezpieczaj urządzenia mobilne

Telefon i tablet powinny być chronione kodem, hasłem lub inną dostępną metodą uwierzytelniania. Warto również korzystać z funkcji umożliwiających odnalezienie, zablokowanie lub zdalne usunięcie danych z utraconego urządzenia.

CHROŃ SWOJE DANE OSOBOWE

1. Nie przekazuj więcej danych, niż jest to konieczne

Przed podaniem danych osobowych zastanów się, czy są one rzeczywiście potrzebne do realizacji danej usługi. Szczególną ostrożność należy zachować przy przekazywaniu skanów lub zdjęć dokumentów tożsamości oraz innych informacji, które mogą zostać wykorzystane do podszywania się pod inną osobę.

2. Zastrzeż numer PESEL

Zastrzeżenie numeru PESEL może ograniczyć ryzyko wykorzystania danych do określonych rodzajów nadużyć. Można to zrobić za pośrednictwem oficjalnych usług administracji publicznej, w tym aplikacji mObywatel.

3. Rozważ uruchomienie alertów dotyczących prób wykorzystania Twoich danych

Dostępne usługi powiadamiania o określonych zdarzeniach związanych z wykorzystaniem danych mogą pomóc szybciej zareagować na próbę oszustwa lub wyłudzenia.

Centrum Obywatelskie Centrum C 10
os. Centrum C 10, 31-931 Kraków
e-mail: c10@ipp.expert
tel./SMS: 578 562 000

BEZPIECZNIE KORZYSTAJ ZE SZTUCZNEJ INTELIGENCJI

1. Nie przekazuj do narzędzi AI poufnych danych bez wcześniejszej oceny ryzyka

Przed przesłaniem informacji do narzędzia wykorzystującego sztuczną inteligencję sprawdź, czy zawierają one dane osobowe, informacje poufne, tajemnice organizacji, dane beneficjentów, pracowników, kontrahentów lub inne informacje, których nie należy udostępniać podmiotom zewnętrznym.

2. Anonimizuj lub pseudonimizuj dane

Jeżeli do wykonania zadania nie są potrzebne prawdziwe dane, usuń informacje umożliwiające identyfikację konkretnych osób lub zastąp je neutralnymi oznaczeniami. Samo zastąpienie imienia i nazwiska może jednak nie wystarczyć, jeżeli pozostałe informacje nadal pozwalają zidentyfikować daną osobę.

3. Sprawdź zasady przetwarzania danych przez wykorzystywane narzędzie

Przed korzystaniem z narzędzia AI w pracy organizacji warto sprawdzić m.in. warunki korzystania z usługi, ustawienia prywatności oraz zasady dotyczące przechowywania i wykorzystywania przekazywanych informacji.

WERYFIKUJ INFORMACJE PUBLIKOWANE W INTERNECIE

1. Sprawdzaj źródła informacji

Nie każda informacja, zdjęcie, nagranie lub wypowiedź publikowana w Internecie jest prawdziwa. Szczególną ostrożność warto zachować wobec treści wywołujących silne emocje, sensacyjnych wiadomości oraz materiałów zachęcających do natychmiastowego udostępnienia. Przed przekazaniem informacji dalej sprawdź jej źródło, datę publikacji oraz potwierdzenie w innych wiarygodnych źródłach. Rozwój generatywnej sztucznej inteligencji dodatkowo zwiększa znaczenie krytycznej oceny treści cyfrowych – także zdjęć, nagrań audio i materiałów wideo.

Centrum Obywatelskie Centrum C 10
os. Centrum C 10, 31-931 Kraków
e-mail: c10@ipp.expert
tel./SMS: 578 562 000

KORZYSTAJ BEZPIECZNIE Z PŁATNOŚCI ELEKTRONICZNYCH

1. Stosuj bezpieczne i odpowiednio zabezpieczone metody płatności

Podczas płatności elektronicznych korzystaj z zaufanych aplikacji i usług oraz każdorazowo sprawdzaj dane transakcji przed jej zatwierdzeniem. Nie potwierdzaj operacji, której samodzielnie nie zainicjowałeś lub której celu nie rozumiesz.

REAGUJ NA INCYDENTY

1. Nie ignoruj podejrzanych zdarzeń

Nietypowa próba logowania, wiadomość o zmianie hasła, której nie wykonywałeś, podejrzany SMS, nieznana transakcja czy wiadomość wysłana z Twojego konta bez Twojej wiedzy mogą świadczyć o incydencie bezpieczeństwa. W takiej sytuacji należy możliwie szybko podjąć odpowiednie działania, m.in. zmienić dane logowania, zabezpieczyć konto oraz skontaktować się z właściwą instytucją lub usługodawcą.

2. Zgłaszaj podejrzane wiadomości i strony

Podejrzane strony internetowe, wiadomości SMS oraz inne próby oszustwa można zgłaszać do właściwych instytucji zajmujących się cyberbezpieczeństwem, w tym CERT Polska. W przypadku podejrzanych wiadomości dotyczących bankowości, płatności lub konkretnej usługi warto również poinformować daną instytucję.

CYBERBEZPIECZEŃSTWO TO PROCES

Bezpieczeństwo cyfrowe nie jest jednorazowym działaniem. Technologie i sposoby działania cyberprzestępców stale się zmieniają, dlatego stosowane zabezpieczenia warto regularnie przeglądać i aktualizować. Największe znaczenie mają **świadomość zagrożeń, dobre nawyki oraz konsekwentne stosowanie podstawowych zasad bezpieczeństwa**.

Kraków
ZADANIE PUBLICZNE FINANSOWANE ZE ŚRODKÓW MIASTA KRAKOWA

Centrum Obywatelskie Centrum C 10
os. Centrum C 10, 31-931 Kraków
e-mail: c10@ipp.expert
tel./SMS: 578 562 000

Nie trzeba wdrażać wszystkich rozwiązań jednocześnie. Każde dodatkowe zabezpieczenie może ograniczyć ryzyko utraty danych, przejęcia konta lub innego incydentu.

Zacznij od podstaw, wdrażaj kolejne rozwiązania i regularnie sprawdzaj poziom bezpieczeństwa swojego cyfrowego środowiska.