Dobre praktyki bezpieczeństwa poświadczeń

Nie udostępniaj loginów ani haseł - Twoje dane to Twoja odpowiedzialność.

Udostępnianie danych uwierzytelniających stanowi poważne zagrożenie dla bezpieczeństwa użytkowników oraz organizacji. Poświadczenia do systemów, poczty oraz innych zasobów powinny być traktowane jako informacje poufne i chronione.

Przekazanie loginu i hasła innej osobie, świadomie lub w wyniku oszustwa, może prowadzić do nieautoryzowanego dostępu, naruszenia poufności danych, przejęcia kont czy kradzieży tożsamości. Każdy użytkownik jest odpowiedzialny za ochronę swoich poświadczeń i nie powinien udostępniać ich osobom trzecim.

Dobre praktyki bezpieczeństwa poświadczeń

1. *Nigdy nie udostępniaj swoich loginów ani haseł*
   - 1.1. Nie podawaj ich współpracownikom – w razie potrzeby istnieją bezpieczne sposoby nadania uprawnień.
   - 1.2. Nie wpisuj ich w e-mailach ani innych komunikatorach.
   - 1.3. Nie zapisuj ich na kartkach ani plikach tekstowych na komputerze czy smartfonie.

2. *Używaj silnych i unikalnych haseł*
   - 2.1. Hasło powinno składać się z minimum 16 znaków.
   - 2.2. Powinno zawierać wielkie i małe litery.
   - 2.3. Hasło powinno zawierać przynajmniej jeden znak specjalny (np. !, @, #, $, %, &).
   - 2.4. Nie używaj tego samego hasła w różnych usługach i serwisach – dla każdej usługi powinno być utworzone konto z oddzielnym, unikalnym hasłem.
   - 2.5. Natychmiast zmień hasło, jeśli tylko podejrzewasz naruszenie bezpieczeństwa.

3. *Korzystaj z menedżera haseł*
   - 3.1. Menedżer bezpiecznie przechowuje hasła.
   - 3.2. Generuje silne i unikalne hasła.

4. *Włącz uwierzytelnianie wieloskładnikowe (MFA)*
   - 4.1. Nie polegaj na kodach SMS, jeśli dostępne są bezpieczniejsze rozwiązania typu: Google Authenticator, Microsoft Authenticator czy klucze U2F.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

5. *Bądź czujny na oszustwa oraz phishing*
   5.1. Nie klikaj w podejrzane linki w e-mailach i wiadomościach.
   5.2. Sprawdzaj adresy stron logowania – atakujący mogą podrobić stronę banku oraz innych organizacji.
   5.3. Nigdy nie podawaj danych logowania przez telefon, e-mail ani czat – administratorzy nigdy o to nie proszą.

6. *Loguj się tylko z bezpiecznych miejsc*
   6.1. Korzystaj z zaufanych urządzeń – nie loguj się na konta służbowe z czyjegoś komputera.
   6.2. Unikaj publicznych sieci Wi-Fi. Jeśli musisz się zalogować, korzystaj z VPN.

7. *Zgłaszaj podejrzane sytuacje*
   7.1. Jeśli otrzymasz podejrzany e-mail, telefon lub wiadomość – natychmiast skontaktuj się z działem IT.
   7.2. Zgłaszaj nietypowe aktywności na swoich kontach oraz sprzęcie.

Zagrożenia wynikające z udostępniania danych uwierzytelniających

Niestosowanie się do zasad bezpieczeństwa dotyczących udostępniania loginów i haseł może prowadzić do poważnych konsekwencji, takich jak:

1. *Przejęcie konta*
   Osoba, której zostaną udostępnione dane, może zmienić hasło i całkowicie uniemożliwić dostęp do konta.

2. *Utrata wrażliwych danych*
   Cyberprzestępcy mogą uzyskać dostęp do poczty elektronicznej, plików oraz systemów firmowych, co może prowadzić do wycieku informacji.

3. *Oszustwa finansowe*
   W przypadku przejęcia konta bankowego lub służbowego, atakujący może dokonywać nieautoryzowanych transakcji na nazwisko poszkodowanego.

4. *Konsekwencje przejęcia konta*
   Wykorzystanie przejętego konta do phishingu lub innych cyberprzestępstw może skutkować konsekwencjami dla osoby, której konto zostało skompromitowane.

5. *Problemy prawne i zawodowe*
   Udostępnienie hasła wbrew zasadom bezpieczeństwa firmy może skutkować konsekwencjami służbowymi, a w niektórych przypadkach nawet prawnymi.

Pojedyncza sytuacja może prowadzić do utraty dostępu do konta oraz narażenia bezpieczeństwa instytucji. Udostępnienie loginu i hasła, nawet na krótki czas, może skutkować utratą kontroli nad kontem, naruszeniem danych organizacji oraz konsekwencjami prawnymi.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706