

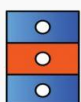
Ochrona danych i bezpieczeństwo w sieci

Ochrona danych w naszej organizacji

Zawsze!



Blokuj komputer opuszczając miejsce pracy



Przechowuj dokumenty zawierające dane osobowe w zamknięciu



Pliki zawierające chronione informacje przechowuj w zabezpieczonej aplikacji



Nie zostawiaj kluczy w zamkach mebli, w których przechowywane są dane osobowe



Dwa razy sprawdź odbiorców wiadomości e-mail przed jej wysłaniem



Regularnie zmieniaj hasło dostępu do systemu i poczty



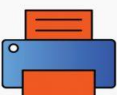
Regularnie czyść folder „Usunięte elementy” w poczcie i na pulpicie



Przeglądaj i aktualizuj wszystkie dane, regularnie usuwaj przeterminowane elementy



Aktualizuj program antywirusowy na swoim komputerze i urządzeniu mobilnym



Pilnuj swoich wydruków i kserokopii

Nigdy!



Nie zostawiaj dokumentów zawierających dane osobowe: na biurku lub w miejscach niezabezpieczonych



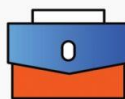
Nie wyrzucaj żadnych dokumentów do kosza – zniszcz je w niszczarce



Nie pobieraj żadnych programów do przechowywania danych osobowych



Nie przechowuj danych osobowych na dyskach lokalnych w laptopie czy dyskach sieciowych ogólnodostępnych



Nie twórz kopii zapasowych dokumentów zawierających dane osobowe i nie wynos ich poza organizację



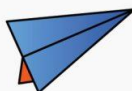
Nie używaj niezasyfrowanych pamięci przenośnych do przechowywania danych osobowych



Nie korzystaj z niezabezpieczonych stron, które do zalogowania wymagają podania danych osobowych



Nie korzystaj z publicznego WiFi do połączenia z pocztą firmową i dyskami zawierającymi dane osobowe



Nie wysyłaj danych osobowych w niezasyfrowanych załącznikach e-mail. Kod odblokowujący plik przesyłaj osobno



Nie przekazuj telefonicznie danych osobowych jeśli nie możesz zweryfikować rozmówcy

Ochrona danych i bezpieczeństwo w sieci

10

Kroków do ochrony przed Phishingiem

Co to jest Phishing?

To praktyka wysyłania wiadomości e-mail, które wydają się pochodzić z renomowanych źródeł w celu wywarcia wpływu lub pozyskania danych osobowych.

Przestrzegając kilku prostych zasad, skutecznie uchronisz się przed kradzieżą haseł, numerów kart kredytowych, danych kont bankowych, pieniędzy i innych poufnych informacji.

Nie klikaj nieznanych linków!

Jeżeli wiadomość zawiera link, najedź na niego kursorem i sprawdź, gdzie faktycznie prowadzi. Nigdy nie klikaj linku, jeśli opis strony wzbudza podejrzenie.

Dokładnie sprawdzaj pisownię!

Jeśli wiadomość zawiera dużo błędów stylistycznych, ortograficznych oraz literówek to powinna wzbudzić Twoją czujność.

Nie działaj pochopnie!

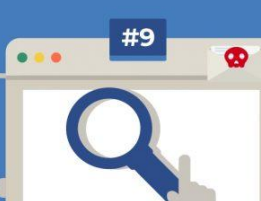
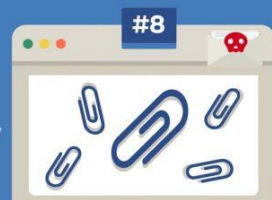
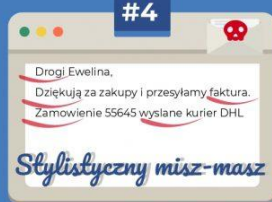
Nigdy dobrowolnie nie odpowiadaj na wiadomości, które próbują na Ciebie wywrzeć presję działania! Większość wiadomości phishingowych zachęca np. do ponownego wpisania hasła.

Uważaj na załączniki!

Cyberprzestępcy uwielbiają wykorzystywanie załączników do przesyłania szkodliwych plików. Nie otwieraj nieznanych plików.

Aktualizuj wiedzę o zagrożeniach!

Twój dział IT powinien na bieżąco informować Cię o najnowszych zagrożeniach. Zgłaszaj wszystkie naruszenia bezpieczeństwa.



Nie ufaj nadawcy wiadomości!

Nie zawsze osoba, której podpis znajdziesz w wiadomości mailowej, to ta za którą się podaje. Dokładnie sprawdź adres mailowy i zweryfikuj nadawcę wiadomości.

Zwróć uwagę na zwrot grzecznościowy!

Forma grzecznościowa "Drogi kliencie" lub "Drogi <automatycznie wypełnione imię>" może wskazywać na phishing. Ktoś kto będzie się chciał z Tobą skontaktować uczciwie, użyje poprawnych form imiennych.

Czy wiadomość zawiera prośbę o podanie danych osobowych?

Wiarygodni nadawcy nigdy nie proszą o podanie prywatnych danych w niezasyfrowanej wiadomości mailowej.

Zwróć uwagę bezpieczeństwo strony!

Bądź pewny, że każda odwiedzana strona ma ważny certyfikat SSL, lub przed adresem strony pojawia się symbol zamkniętej kłódki.

Bądź podejrzliwy!

Jeśli jakiś element wiadomości wygląda podejrzanie to ją zignoruj. Zgłaszaj wszelkie nieprawidłowości.

Zapamiętaj!

Jeśli jesteś pewien, że Twój system operacyjny jest regularnie aktualizowany przy pomocy łątek i uaktualnień pobranych ze strony producenta oraz zabezpieczony programem antywirusowym, zastosuj dodatkowo dobre praktyki i ustrzeż się przed podstępny cyberatakami.

Ochrona danych i bezpieczeństwo w sieci