Janusz Wyspiański – Inspektor Ochrony

Zasady ochrony Informacji - cyberbezpieczeństwo

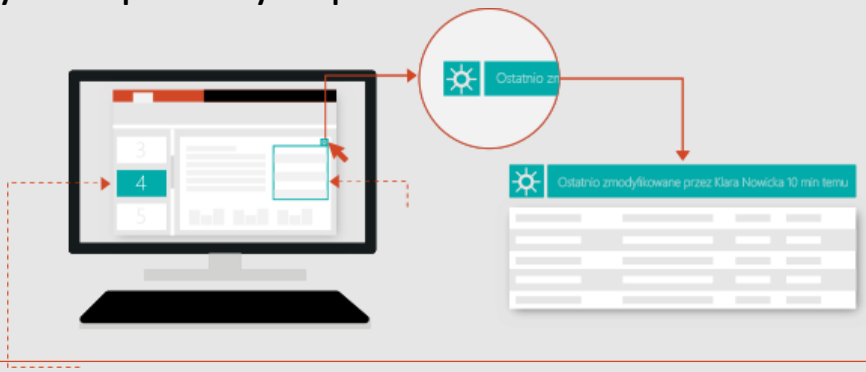
Dzięki szkoleniu dowiesz się:

- **Jak tworzyć bezpieczne hasła i zarządzać nimi,**
- **Jak właściwie korzystać z poczty służbowej i zasobów internetu,**

- **Jak bezpiecznie korzystać z mediów społecznościowych**
- **Jak rozpoznawać zagrożenia cyberbezpieczeństwa – phishing – i właściwie reagować.**

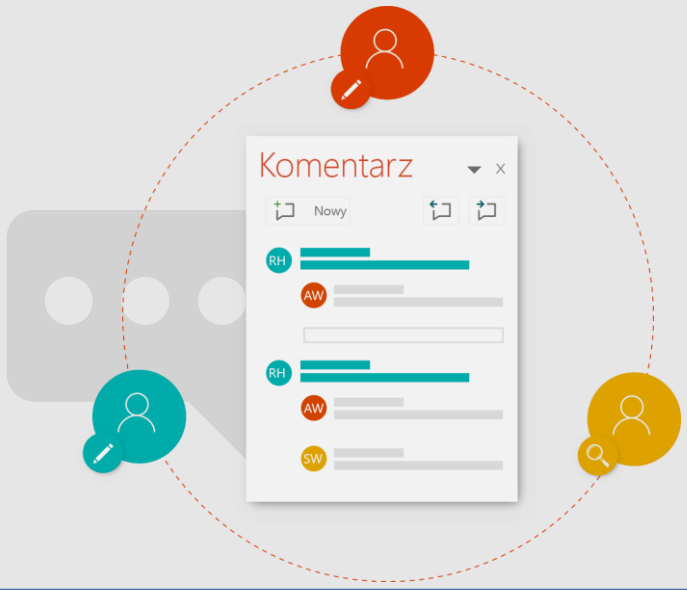
Jaki jest sens RODO?

Do momentu wejścia w życie RODO w Unii Europejskiej nie funkcjonował spójny system ochrony danych osobowych, co – biorąc pod uwagę swobodę przepływu osób, usług i kapitału – jest ważne dla ochrony podstawowych praw i wolności jej obywateli. Dla przeciętnego Kowalskiego ochrona danych osobowych już od dawna nie sprowadza się do walki z natrętnym telemarketingiem. Giganci technologiczni są już bowiem w stanie, poprzez operacje na naszych danych, wpływać na nasze wybory polityczne czy ceny biletów lotniczych kupowanych przez Internet.



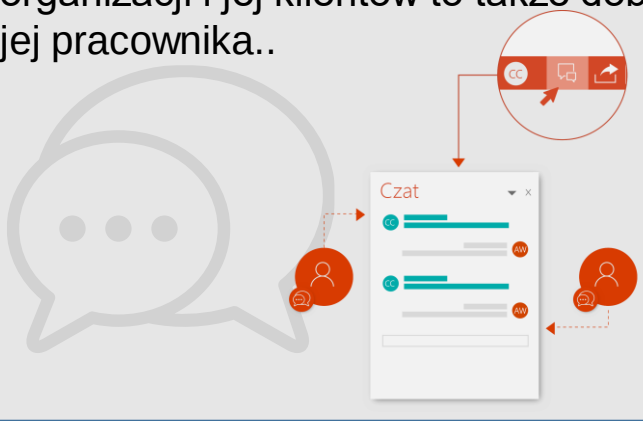
Obowiązki Administratora Danych Osobowych

Oprócz zapewnienia informacji na temat przetwarzania, akt ten zobowiązuje też administratorów danych do stosowania środków technicznych i organizacyjnych, które zapewnią odpowiedni poziom bezpieczeństwa.



Współodpowiedzialność

RODO wymusza stałe dostosowywanie organizacji do zmieniającej się rzeczywistości – źródłem naruszenia może być każdy człowiek i każdy zasób przetwarzający dane osobowe. Utrata reputacji lub konieczność zapłaty wysokich odszkodowań czy kar finansowych mogłaby odbić się na całym zespole pracowników. Jeśli pracownik naruszy swoje obowiązki musi liczyć się także ze swoją odpowiedzialnością. Dlatego dobro organizacji i jej klientów to także dobro jej pracownika..



Wydawać by się mogło, że ustawienie monitora lub miejsce przechowywania dokumentów, nie ma dużego wpływu na funkcjonowanie firmy.
A jednak służbowe biurko jest wyjątkowym źródłem wiedzy o organizacji.
Brak odpowiednich środków bezpieczeństwa, a także lekkomyślne zachowania zarówno zwykłych pracowników, jak i kadry zarządzającej mogą przyczynić się do niezamierzonego udostępnienia cennych informacji.

Najczęściej występujące typy incydentów:

- **wysyłka wiadomości e-mail pod błędny adres,**
- **zgubienie laptop,**
- **pozostawienie niezabezpieczonych dokumentów,**
- **praca w domu przy dostępie rodziny i znajomych na komputerach niezabezpieczonych antywirusem, bez aktualizacji bezpieczeństwa**

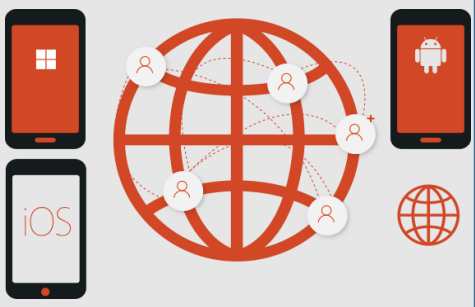
Polityka haseł:

Jesteś daleko od swojego biurka? Szybko wprowadzisz zmiany na telefonie lub laptopie - ZAWSZE ZABEZPIECZ DOSTĘP DO KOMPUTERA HASŁEM Z AUTOMATYCZNYM WYLOGOWYWANIEM.

Najczęstszym źródłem wycieku haseł jest ich właściciel.

Dlatego zawsze stosuj się do poniższych zaleceń:

- **nie zapisuj haseł i nie umieszczaj ich w miejscach dostępnych dla innych osób,**
- **nie stosuj haseł łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imion, numerów telefonu, dat urodzenia itp.,**
- **nie używaj tych samych haseł w różnych systemach operacyjnych i aplikacjach oraz w życiu służbowym i prywatnym,**



- nie zapisuj haseł „na stałe” oraz nie wykorzystuj opcji autozapamiętywania haseł (np. w przeglądarkach internetowych),
- nie twórz haseł w sposób przewidywalny, np. kolejno: HasłoLipiec1!, HasłoSierpień1!, HasłoWrzesień1!
- stosuj „szyfry” polegające np. na: złożeniu hasła z pierwszych liter wyrazów składających się na jakieś zdanie (np. OMGzzh* od Oh My God znowu zapomniałem hasła* czy GJSkś* od Gdzie Jest Słonko kiedy śpi*).

Poczta elektroniczna:

- Niedozwolone jest wykorzystywanie prywatnej poczty elektronicznej do celów służbowych. Dotyczy to zarówno wysyłania dokumentów i danych na swoje skrzynki prywatne, jak i podawania klientom i kontrahentom swoich adresów prywatnych w celu wymiany korespondencji.

- Ponadto podczas korzystania z poczty nie powinno otwierać się załączników takich jak programy wykonywalne (np. z rozszerzeniem .exe), gdyż mogą one zawierać szkodliwe oprogramowanie

PAMIĘTAJ !!!

- **Pracodawca, jeżeli wcześniej poinformuje o tym swoich pracowników i współpracowników (w sposób określony w kodeksie pracy), ma prawo do monitorowania poczty wychodzącej i przychodzącej ze służbowej skrzynki pocztowej oraz przeglądanych stron internetowych.**

Zasady przesyłania korespondencji masowej

Częstym naruszeniem bezpieczeństwa danych w masowej korespondencji elektronicznej jest ujawnienie poszczególnych odbiorców wiadomości. Przy masowej wysyłce elektronicznej korespondencji (np. mailingu reklamowym) nie wolno udostępniać innym listy mailingowej, zawierającej dane osobowe pozostałych adresatów takiej wiadomości, ponieważ podlegają one ochronie.

W przypadku wysyłania korespondencji do większej liczby osób poza organizację należy dbać o to, aby osoby, do których skierowana jest tego typu korespondencja, nie miały możliwości zapoznania się z danymi pozostałych adresatów wiadomości – nie tylko ich imionami i nazwiskami, lecz także adresami e-mail

Wysyłając korespondencję masową poza organizację, tak aby adresy odbiorców nie były widoczne adresy należy wprowadzać w pole:

UDW: (ukryte do wiadomości).

Używanie adresów służbowych w celach prywatnych

Rejestrowanie się na stronach internetowych do celów prywatnych przy pomocy służbowych adresów e-mail jest niewskazane. Powszechnie udostępniony adres służbowy pozwala przestępcom na zidentyfikowanie pracowników Twojej organizacji i ułatwia im stworzenie bazy danych adresów, które mogą stanowić przedmiot potencjalnego ataku.

Należy pamiętać, że w przypadku adresów służbowych celem ataku nie jest pojedynczy pracownik, ale cała organizacja, która przetwarza dane wielu osób, w związku z czym dane te powinny podlegać szczególnej ochronie.

- **Pamiętaj też, że używając służbowego adresu, reprezentujesz swoją organizację na zewnątrz. Przykładowo, publikując opinie na GoldenLine czy LinkedIn, robisz to jako przedstawiciel organizacji, która Cię zatrudnia – czyń to z rozsądkiem.**

Fałszywe wiadomości e-mail (phishing)

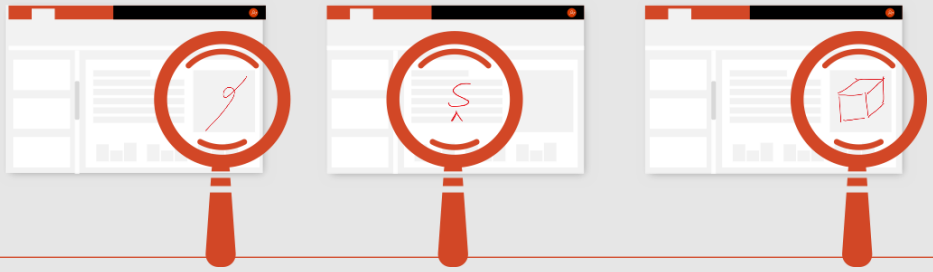
Od dłuższego już czasu użytkownicy Internetu otrzymują e-maile łudząco podobne do wysyłanych przez Pocztę Polską, firmy kurierskie czy telekomunikacyjne. Spreparowane wiadomości często zawierają załącznik z oprogramowaniem, którego otworzenie powoduje zainfekowanie komputera, a w konsekwencji – wyłudzenie m.in. danych uwierzytelniających do kont bankowych czy zaszyfrowanie zawartości Twojego komputera lub serwera służbowego (bywa, że pojawia się żądanie okupu w zamian za jego odszyfrowanie).

Dlatego zwracaj baczną uwagę na otrzymywane wiadomości:

- ❑ przeczytaj uważnie treść e-maila, przyjrzyj się formie – jeśli masz wątpliwości, porównaj ją z innymi e-mailami od tego samego nadawcy,
- ❑ zachowaj czujność w przypadku wiadomości w jakikolwiek sposób związanych z kwestiami finansowymi,
- ❑ przed kliknięciem w link sprawdź, dokąd prowadzi – jeśli odsyła do formularza, w którym trzeba podać ważne dane, zachowaj ostrożność,
- ❑ szczególnie uważaj na e-maile, w których nadawca straszy Cię konsekwencjami lub zbyt wiele obiecuje,
- ❑ nie otwieraj załączników, które budzą Twoją wątpliwość,
- ❑ zwracaj uwagę na samą treść wiadomości, jej styl oraz jej poprawność językową – błędy mogą spowodować zapalenie się czerwonej lamki, gdyż wiadomości tworzone przez profesjonalne podmioty są co do zasady profesjonalnie sformułowane.
- ❑ **W razie otrzymania podejrzanej wiadomości e-mail pamiętaj o bezzwłocznym powiadomieniu Informatyka w swojej organizacji. !!!**

Przeglądanie zasobów Internetu:

- Podczas korzystania z przeglądarek internetowych należy zwracać uwagę na nietypowe rzeczy, które dzieją się podczas pracy. Najbardziej popularne, nieautoryzowane zmiany mogą powodować: wyświetlające się okienka z reklamami, zmianę wyglądu strony, podejrzane linki, reklamy wyświetlające się na stronach internetowych bez możliwości ich zamknięcia.



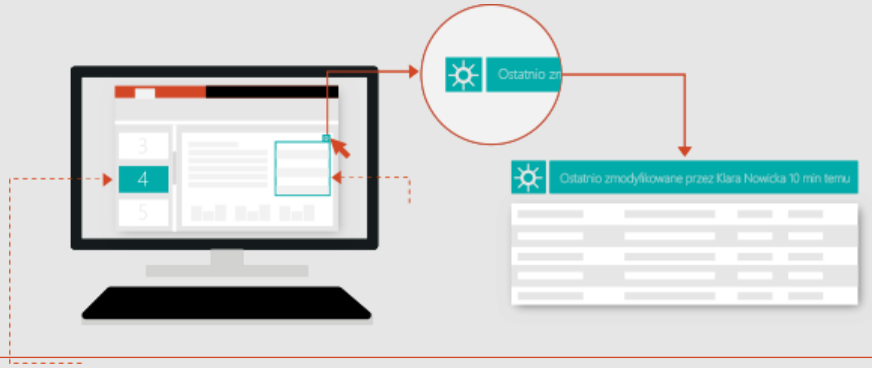
Wypowiedzi na portalach i forach

- **Niedozwolone jest publikowanie na portalach internetowych danych osobowych stanowiących informację służbową uzyskaną podczas pracy, o ile nie leży to w zakresie obowiązków pracownika.**

- **Niewskazane jest publikowanie wiadomości prywatnych (z zastrzeżeniem ograniczonego wykorzystania dostępu do Internetu do celów prywatnych) na stronach internetowych, na których publicznie widoczny jest adres IP Twojego pracodawcy.**

Test sprawdzający zdobytą wiedzę:

Test składa się z czterech pytań. Do każdego z nich dołączono cztery możliwe odpowiedzi. Każde z pytań jest wielokrotnego wyboru, co oznacza, że jedna odpowiedź, dwie, trzy lub wszystkie mogą być poprawne.



PYTANIE 1

Hasło to:

- Im mniej jest związane z osobą je stosującą, tym trudniejsze do złamania.
- Im więcej różnorodnych znaków zawiera, tym jest trudniejsze do złamania.
- Składające się z samych cyfr jest wystarczająco mocne. Nie można złamać takiego hasła.
- Powinno być krótkie, gdyż dzięki temu łatwo je zapamiętać.

PYTANIE 2

Wskaż najtrudniejsze hasło do złamania:

- ❑ Qwerty
- ❑ Bożena001
- ❑ QwE456PoI654.
- ❑ Qaz123.

PYTANIE 3

Przesyłanie dokumentacji służbowej na prywatny adres poczty elektronicznej jest:

- ❑ **Dopuszczalne za zgodą przełożonego.**
- ❑ **Całkowicie zabronione.**
- ❑ **Dopuszczalne – przecież muszę dokończyć pracę w domu.**
- ❑ **Dopuszczalne – dopóki nikt o tym nie wie.**

PYTANIE 4

Kiedy pracodawca może monitorować służbową pocztę pracownika?

- ❑ **Po ukończeniu przez pracownika szkolenia z ochrony danych osobowych.**
- ❑ **Po wcześniejszym poinformowaniu o tym pracownika.**
- ❑ **Zaraz po podpisaniu umowy.**
- ❑ **Gdy pracodawca zakupi odpowiednie oprogramowanie.**