Uniwersytet Jana Kochanowskiego w Kielcach

Zasady bezpiecznej pracy zdalnej.

Szkolenie dla pracowników

Na podstawie materiałów udostępnionych przez odo24.pl

Szkolenie dostarcza informacji na temat:

- bezpiecznej pracy z urządzeniami mobilnymi oraz dokumentacją papierową;
- właściwego korzystania z poczty służbowej i zasobów Internetu;
- zasad komunikowania się poza siedzibą pracowdawcy;
- niebezpieczeństw związanych z phishingiem.

Szkolenie składa się z 12 merytorycznych slajdów.
Na odbycie szklenia zarezerwuj sobie ok. 15 minut.

Wprowadzenie do bezpieczeństwa informacji

Wydawać by się mogło, że miejsce pracy na ma dużego wpływu na bezpieczeństwo informacji.

Jednak brak odpowiednich środków bezpieczeństwa, a także nieprzemyślane zachowania pracowników i osób z ich otoczenia (np. domowników czy współlokatorów) mogą przyczynić się do niezamierzonego udostępnienia cennych informacji.

Najczęściej występujących typów incydentów zwykle można uniknąć, jeśli pracownik nie popełni błędu takiego jak:

- zbubienie laptopa,
- pozostawienie niezabezpieczonych dokumentów i urządzeń,
- praca w domu na urządzeniach dostępnych dla rodziny, znajomych itd.

Dzięki temu modułowi szkolenia dowiesz się, jak w prosty sposób podnieść poziom bezpieczeństwa podczas pracy w domu.

Bezpieczna praca poza siedzibą UJK

Na pracy zdalnej należy zachować szczególną ostrożność podczas prowadzenia rozmów w miejscach, **które nie gwarantują zachowania poufności**. W ich trakcie może bowiem dochodzić do wymiany informacji poufnych będących własnością pracodawcy, w tym danych osobowych.

Nie udostępniaj urządzenia, na którym pracujesz osobom nieupoważnionym: domownikom, współlokatorom lub innym osobom postronnym.

Podczas pracy zdalnej korzystaj tylko z zabezpieczonej domowej sieci lub z połączenia udostępnionego przez Ciebie (hotspot z Twojego telefonu).

Jeżeli urządzenie lub dokumenty, na których pracujesz, ulegną zniszczeniu lub zostaną zgubione, bezzwłocznie poinformuj o tym Inspektora Ochrony Danych. **Takie zdarzenie może okazać się naruszeniem ochrony danych osobowych.**

Stosowanie się do przyjętych przez pracodawcę standardów w zakresie bezpieczeństwa

Pamiętaj, że jesteś zobowiązany do stosowania zabezpieczeń wdrożonych przez Uniwersytet.

Są to działania takie jak:

- łączenie się z siecią firmową przy wykorzystaniu szyfrowanego połączenia VPN z zasobami firmowymi (np. serwer plików, poczta elektroniczna, systemy wewnętrzne firmy);
- właściwe ustawienie monitora w celu zachowania poufności informacji wyświetlanych na ekranie komputera;
- aktualizowanie oprogramowania urządzeń, na których pracujesz;
- blokowanie komputera oraz zabezpieczenie dokumentów papierowych, na których pracujesz, w razie oddalenia się od miejsca pracy w ramach pracy zdalnej;
- uporządkowania miejsca pracy po jej zakończeniu, stosowanie "zasady czystego biurka".

Stosowanie się do przyjętych przez pracodawcę standardów w zakresie bezpieczeństwa

Oraz:

- niepodłączanie nośników niewiadomego pochodzenia;
- brak ustawienia zapamiętywania hasła do poczty elektronicznej przez przeglądarkę internetową;
- zainstalowanie programu antywirusowego działającego w tle;
- utrzymanie w tajemnicy danych uwierzytelniających w systemach;
- zaszyfrowanie dysku twardego Twojego komputera.

Pamiętaj o tym, że...

Podczas pracy zdalnej należy zapobiegać udostępnieniu danych osobowych nieuprawnionym podmiotom.

W tym celu:

- nie drukuj dokumentów firmowych w ogólnodostępnych punktach ksero;
- prawidłowo transportuj sprzęt oraz dokumentację wykorzystywaną do pracy zdalnej;
- nie wyrzucaj dokumentów firmowych do śmietnika - przechowuj je do momentu bezpiecznego zniszczenia.

Poczta elektroniczna

Prywatna poczta elektroniczna nie może być wykorzystywana do celów służbowych.
Powinieneś korzystać w tym celu jedynie ze służbowego konta e-mail.

Zalecenia bezpiecznego korzystania z poczty:

- Dane osobowe – nie należy przesyłać danych osobowych w niezabezpieczonej formie (w treści wiadomości)
- Szyfrowanie załączników – do tego celu należy wykorzystać oprogramowanie udostępnione przez pracodawcę. Takim oprogramowaniem może być np. 7zip lub usługa pakietu Office;
- Wysyłanie hasła do pliku osobnym kanałem komunikacji – jeśli wyślemy zaszyfrowany załącznik poprzez pocztę elektroniczną, to hasło do niego powinniśmy podać telefonicznie lub za pomocą SMS-a;
- W miarę możliwości usuwanie wysłanych wiadomości – zmniejszy to skalę rozproszenia danych osobowych;
- Ponadto podczas korzystania z poczty nie należy otwierać załączników z programami wykonywalnymi (np. z rozszerzeniem exe), gdyż mogą zawierać szkodliwe oprogramowanie

Fałszywe wiadomości e-mail (phishing)

Phishing - metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych osobowych), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań.

Spreparowane wiadomości często zawierają załącznik z oprogramowaniem lub link do niego. Otworzenie takiego załącznika powoduje zainfekowanie komputera, a w konsekwencji - wyłudzenie np. danych uwierzytelniających do kont bankowych czy zaszyfrowanie zawartości komputera lub serwera służbowego (bywa, że pojawia się żądanie okupu w zamian za odszyfrowanie).

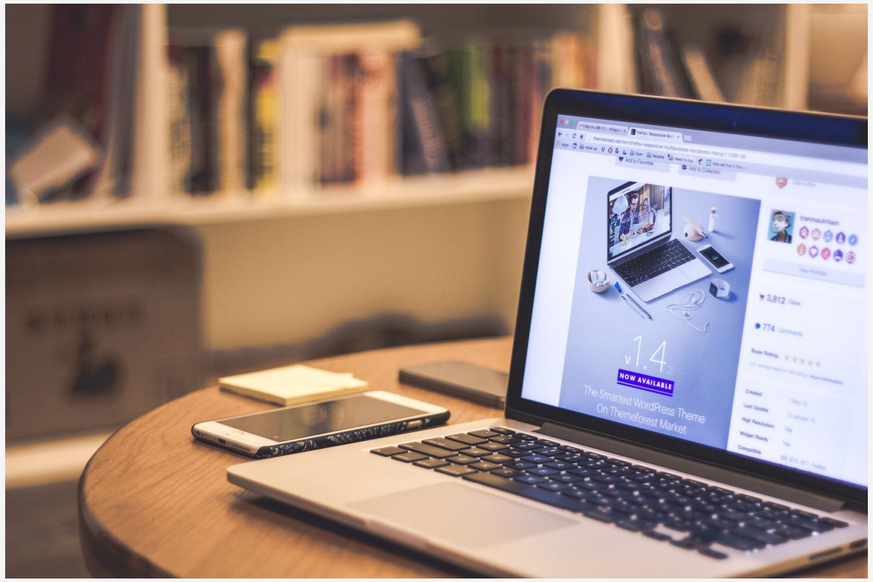
Fałszywe wiadomości e-mail (phishing)

Zwracaj baczną uwagę na otrzymywane wiadomości:

- Przeczytaj uważnie treść e-maila, przyjrzyj się jego formie - jeśli masz wątpliwości, porównaj wiadomość z innymi e-mailami od tego samego nadawcy.
- Zachowaj czujność w przypadku otrzymywania wiadomości w jakikolwiek sposób związanej z kwestiami finansowymi.
- Nie klikaj w podejrzane linki.
- Szczególnie uważaj na e-maile, w których nadawca straszy Cię konsekwencjami lub zbyt wiele obiecuje.
- Nie otwieraj załączników, które budzą Twoją wątpliwość.
- Patrz na treść wiadomości, jej styl oraz poprawność językową - błędy mogą być sygnałem ostrzegawczym, gdyż teksty tworzone przez profesjonalne podmioty są co do zasady prawidłowo sformułowane.
- Dokładnie weryfikuj adres nadawcy.

W przypadku jakichkolwiek wątpliwości co do autentyczności wiadomości e-mail należy ją przesłać na adres: postmaster@ujk.edu.pl lub skontaktować się z Administratorem Systemu Poczty Elektronicznej UJK (41 349 6205, 41 349 6206)

Przeglądanie zasobów Internetu



Podczas korzystania z przeglądarek internetowych należy zwracać uwagę na nietypowe rzeczy, które dzieją się w trakcie pracy. Najczęstsze nieautoryzowane zmiany mogą być powodowane przez: wyświetlające się okienka z reklamami, zmianę wyglądu strony, podejrzane linki, reklamy wyświetlające się na stronach internetowych bez możliwości ich zamknięcia.

W ostatnim czasie w sieci można natrafić na portale, które służą do wyłudzania danych osobowych oraz haseł.

Najważniejsze, aby pamiętać o niepodawaniu tego typu informacji na stronach, których pochodzenia nie jesteśmy pewni.

O braku wiarygodności portalu może świadczyć np. brak szyfrowania SSL (kłódka z lewej strony adresu WWW) lub pojawianie się okienek reklamowych, których nie można zamknąć.

Raportowanie naruszeń

Przez **naruszenie ochrony danych osobowych** należy rozumieć naruszenie bezpieczeństwa, prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Gdy naruszenie ochrony danych osobowych wiąże się z ryzykiem naruszenia praw lub wolności osób fizycznych, po stronie pracodawcy powstaje konieczność zgłoszenia zdarzenia do Prezesa Urzędu Ochrony Danych Osobowych (PUODO). **Takiego zawiadomienia należy dokonać bez zbędnej zwłoki, ale nie później niż w ciągu 72 godzin od stwierdzenia naruszenia.**

Jeżeli naruszenie niesie za sobą wysokie ryzyko naruszenia praw lub wolności osób fizycznych, pracodawca powinien bez zbędnej zwłoki zawiadomić również osobę, której danych osobowych dotyczy to zdarzenie.

Pamiętaj, aby informować Inspektora ochrony Danych UJK o każdej sytuacji, która w Twojej ocenie może być naruszeniem ochrony danych.

Raportowanie naruszeń - przykłady

- nieuprawnione użycie systemu informatycznego (np. włamanie do systemu informatycznego)
- wysłanie e-maila do wielu odbiorców w kopii otwartej
- wykrycie informatycznego urządzenia lub programu służącego do przechwycenia haseł czy danych;
- kradzież albo zagubienie nieszyfrowanego laptopa lub pamięci zewnętrznej (dysku USB), zawierających dane osobowe
- nieprawidłowe zniszczenie dokumentów lub nośników danych (pendrive, płyty CD/DVD)
- porzucenie wydruków dokumentów (szczególnie w dużych ilościach)

Odpowiedzialność

Naruszenie przepisów związanych z ochroną danych osobowych w Uniwersytecie jest zagrożone sankcjami karnymi określonymi w ustawie oraz Kodeksie karnym.

Naruszenie przepisów związanych z ochroną danych osobowych w Uniwersytecie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować zastosowaniem sankcji wynikających z prawa pracy.

Dziękuję za uwagę

Inspektor Ochrony
Danych UJK