UNIWERSYTET WARSZAWSKI

Inspektor Ochrony Danych

Warszawa, 25 listopada 2019 r.

IOD-042-202/2019

Opracowanie: Dominik Ferenc

Bezpieczne korzystanie z urządzeń IT

komputer stacjonarny/ przenośny

- ustaw login i hasło dostępowe do systemu;
- zastosuj pełne szyfrowanie dysków twardych;
- zainstaluj oprogramowanie antywirusowe;
- nie zachowuj loginów i haseł w pamięci przeglądarki;
- korzystaj z różnych haseł dostępu do stron internetowych/aplikacji – wykorzystaj do tego menagera haseł;
- regularnie wykonuj kopie zapasowe (backup danych);
- aktualizuj oprogramowanie;
- sprawdź ustawienia prywatności przeglądarki internetowej;
- nie wykorzystuj urządzeń służbowych do celów prywatnych;
- przechowuj tylko te dokumenty, które są ci niezbędne do realizacji zadań służbowych;
- ograniczaj wgląd osób trzecich w zawartość monitora;
- nie korzystaj z niezabezpieczonych sieci wi-fi;
- nie pozostawiaj komputera bez nadzoru;

ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa
tel.: 22 55 22 042
e-mail: iod@adm.uw.edu.pl

- zachowaj ostrożność przy wypełnianiu formularzy internetowych;
- przenoś i przechowuj sprzęt w sposób bezpieczny;
- korzystaj z uczelnianego VPN'a[1];
- usuwaj dane w sposób trwały;
- nie przekazuj loginów i haseł innym użytkownikom;

smartphone/tablet

- ustaw dostęp do urządzenia za pomocą PIN'u, hasła, znaku graficznego;
- ustaw blokowanie karty SIM za pomocą PIN'u;
- jeśli możesz, ustaw wymazywanie zawartości w przypadku błędnego odblokowywania urządzenia;
- jeżeli nie korzystasz z urządzenia wyłącz dostęp do wi-fi lub bluetooth;
- spisz i zachowaj nr seryjny swojego urządzenia oraz IMEI;
- włącz opcję Find My Device/Find My iPhone;
- ogranicz prawa dostępu aplikacji do treści na telefonie;
- nie ulegaj łatwo komunikatom zmuszającym cię do umożliwienia dostępu aplikacji do zawartości urządzenia;
- pobieraj wyłącznie oprogramowanie pochodzące z legalnych źródeł;
- korzystaj z uczelnianego VPN'a;
- nie korzystaj ze służbowego urządzenia do celów prywatnych;
- regularnie twórz kopie zapasowe (backup danych);
- ograniczaj wgląd w zawartość ekranu urządzenia;
- nie pozostawiaj urządzenia bez nadzoru;
- przechowuj tylko te dane, które są ci niezbędne do pracy;
- zachowaj ostrożność przy wypełnianiu formularzy internetowych;
- usuwaj dane w sposób trwały;
- nie przekazuj loginów i haseł innym użytkownikom;

dysk przenośny

- szyfruj dyski przenośne;
- przenoś tylko te pliki, które są niezbędne do wykonywania zadań służbowych;
- chroń przechowywane pliki za pomocą hasła;
- usuwaj pliki po ustaniu okresu przydatności;
- nie korzystaj z dysków służbowych w celach prywatnych;
- nie pozostawiaj dysków bez nadzoru;
- nie podpinaj dysków do urządzeń niezaufanych;

[1] https://it.uw.edu.pl/pl/uslugi/UslugiInternetVPN/

dysk w chmurze

- jeśli nie musisz, nie przechowuj dokumentów w dyskach chmurowych;
- korzystaj tylko z dysków w chmurze udostępnionych przez uczelnię;
- ogranicz dostęp do dysku tylko dla uprawnionych użytkowników;
- dokumenty zawierające informacje wymagające ochrony przechowuj zabezpieczone hasłem;
- usuwaj pliki po ustaniu okresu przydatności;
- przy logowaniu do dysku w chmurze nie korzystaj z niezabezpieczonych sieci wi-fi.

Jeżeli nie wiesz jak zastosować wskazane ustawienia skontaktuj się z informatykiem!