Luty 2023

Newsletter

Główna Biblioteka Pracy i Zabezpieczenia Społecznego

W pierwszej połowie lutego, w całej Europie i kilku państwa pozaeuropejskich, obchodzony jest Dzień Bezpiecznego Internetu (DBI). Święto zostało ustanowione w 2004 roku przez Komisje Europejską. Jest częścią programu „Safer Internet" realizowanego przez europejską sieć Centrów Świadomości - Insafe.[1] Promują one bezpieczne, efektywne i świadome korzystanie z technologii cyfrowych i komunikacyjnych oraz kształtują kompetencje cyfrowe. Sieć wzywa do współodpowiedzialności za ochronę praw i potrzeb obywateli (ze szczególnym naciskiem na prawa i ochronę dzieci) wraz z rządem, placówkami edukacyjnymi, rodzicami, mediami i wszystkimi innymi odpowiednimi podmiotami. Centra ściśle współpracują z przemysłem, szkołami i rodzinami, aby zniwelować lukę cyfrową między domem a szkołą oraz między pokoleniami.

Polskimi centrami realizującymi program Safer Internet [2] są Fundację Dajemy Dzieciom Siłę [3] (dawniej Fundacja Dzieci Niczyje) oraz NASK [4].

DZIEŃ BEZPIECZNEGO INTERNETU

Czytaj dalej

10 zasad bezpiecznego korzystania z sieci

Bezpieczna praca w sieci to niezwykle istotna sprawa. Lepiej jest zapobiegać niż rozwiązywać zaistniałe problemy. Dodatkowo wyciek służbowych danych lub zainfekowanie sprzęty złośliwym oprogramowaniem wiąże się z odpowiedzialnością finansową lub czasochłonnymi naprawami. Przy okazji Dnia Bezpiecznego Internetu warto przypomnieć kilka uniwersalnych zasad, które zwiększają bezpieczeństwo w Internecie:

1. **Korzystaj z mocnych haseł.** Mocne hasło to kombinacja liter, cyfr i znaków specjalnych. Im więcej znaków w haśle tym jest ono trudniejsze do złamania – najlepiej aby składało się, z co najmniej 8-12 znaków. [5] Do każdego z serwisów i sprzętów należy używać unikalnego hasła. Nie zapisujmy hasła w przeglądarce.
2. **Korzystaj tylko z zaufanych sieci.** Łączenie się z publiczną siecią Wi-Fi, szczególnie tej, która nie jest zabezpieczona hasłem to prosta droga do kradzieży danych.
3. **Stosuj oprogramowanie antywirusowe.** Do pewnego stopnia oprogramowanie antywirusowe stanowi barierę ochronną naszych urządzeń przed niechcianymi szkodliwymi programami. Oprogramowanie antywirusowe podpowie również użytkownikowi, czy dana strona jest bezpieczna i jakie ewentualne zagrożenia tam czekają. Pobrane pliki zawsze będą filtrowane pod kątem szkodliwej zawartości.
4. **Nie otwieraj podejrzanych maili.** Zachowaj czujność! Częstą praktyką internetowych złodziei jest podszywanie się pod znane firmy, banki i instytucje, od których często dostajemy maile - tzw. phishing.
5. **Aktualizuj przeglądarkę, system operacyjny i oprogramowanie.** Dzięki regularnemu dbaniu o higienę swojego sprzętu, dłużej zachowasz jego sprawność i zadbasz o bezpieczeństwo danych. Każdy system ma swoje luki, które są chętnie wykorzystywane przez cyberprzestępców. Ci uczą się obchodzić zabezpieczenia. Użytkownicy posiadający stare wersje oprogramowania i nieposiadający łatek bezpieczeństwa, stają się łatwym celem hackerów. Dlatego bycie na bieżąco z aktualizacjami, to utrudnianie pracy złodziejom.
6. **Odwiedzaj jedynie bezpieczne strony.** Jedną z podstawowych form zadbania o swoje bezpieczeństwo w Internecie jest odwiedzanie stron, które posiadają certyfikat bezpieczeństwa. Kiedy odwiedzimy stronę niebezpieczną, przeglądarka da nam o tym znać. Certyfikat bezpieczeństwa zapewnia szyfrowanie danych między użytkownikiem, a serwerem strony. To znaczy, że dane, które podamy na stronie względnie trudno przechwycić.

7. **Nie pobieraj programów z nielegalnych źródeł.** Pobierając programy z nielegalnych źródeł, możesz narazić swojego pracodawcę na szereg kar. Instalując różnego rodzaju programy czy gry, możesz łatwo zainfekować komputer wirusami czy też trojanami.
8. **Nie podawaj swoich danych osobowych.** Im mniej Twoich danych osobowych w sieci, tym lepiej. Nawet banalna informacja, może posłużyć przestępcom do ataku. Mogą wykorzystać je np. do phishingu.
9. **Blokuj ekran, gdy odchodzisz od komputera.** Nikt nie powinien mieć wglądu do Twoich służbowych informacji!
10. **Twórz kopie zapasowe.** W wyniku awarii komputera, ale także cyberataku, możesz bezpowrotnie stracić swoje dane. Zawsze staraj się utworzyć kopie zapasowe najważniejszych dla Ciebie rzeczy (plików, zdjęć, kontaktów) w różnych miejscach. Możesz wykorzystać wirtualną chmurę lub pamięć zewnętrzną (dysk przenośny, pendrive).

Źródła i linki do dokumentów elektronicznych

1. Komisja Europejska: Kształtowanie cyfrowej przyszłości Europy. [https://digital-strategy.ec.europa.eu/pl]
2. Polskie Centrum Programu Safer Internet. [https://www.saferinternet.pl/]
3. Fundacja Dajemy Dzieciom Siłę. [https://fdds.pl/]
4. Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy. [https://www.nask.pl/]
5. Wikipedia: Siła haseł. https://pl.wikipedia.org/wiki/Has%C5%82o_(kryptografia)#Si%C5%82a_hase%C5%82

Nowości w GBPiZS

Przegląd prasy

30 stycznia – 05 lutego 2023 r.
06 – 12 luty 2023 r.
13 – 19 luty 2023 r.
20 – 26 luty 2023 r.
27 lutego – 05 marca 2023 r.

Wykaz nabytków książkowych Zbiorów Pracy i Zabezpieczenia Społecznego

Nowości Działu Zbiorów dla Niewidomych

Od 1 lutego 2023 r. wypożyczalnie **Działu Zbiorów dla Niewidomych** Głównej Biblioteki Pracy i Zabezpieczenia Społecznego **we wtorki są czynne do godz. 18.00.**
Prosimy o telefoniczne umawianie wizyty pod numerami: 22-635-83-45 oraz 22-831-22-71.

Lokalizacja i kontakt

Dział Zbiorów dla Niewidomych
ul. Konwiktorska 7
00-216 Warszawa (Śródmieście)

tel.: 22 635-83-45
email: dw@dzdn.pl

Dział Zbiorów Pracy i Zabezpieczenia Społecznego
ul. Zabraniecka 8L
03-872 Warszawa (Targówek Fabryczny)
Dojazd do przystanku „Zabraniecka 02”
autobusami: **138, 338**

tel.: (+48) 509-787-563
e-mail: sekretariat@gbpizs.gov.pl