- Projekt **„Szkolenia dla kadry edukacji szkolnej w wymiarze europejskim”** realizowany w Zespole Szkół Kształcenia Ustawicznego od 01.10.2018 do 29.02.2020, finansowany ze środków Europejskiego Funduszu Społecznego, Program Operacyjny Wiedza Edukacja Rozwój (POWER) w ramach projektu: „Ponadnarodowa Mobilność Kadry Edukacji Szkolnej” – nr POWERSE-2018-1-PL01-KA101-049092.
- Dofinansowanie projektu z UE: 84 428,56 PLN

Bezpieczeństwo w Internecie

Internet jest narzędziem przydatnym do nauki, pracy i zabawy. Niestety, jak każde narzędzie może być używane do dobrych i złych działań. Warto wiedzieć jakie występują w nim zagrożenia i jak się przed nimi chronić.

Niektóre zagrożenia w Internecie:

- **Hejt**
- **Cyberprzemoc**
- **Wirusy**
- **Fałszywe profile**
- **Źle zabezpieczone strony sklepów internetowych**

Hejt

W sieci można spotkać nieprzyjemne, obraźliwe wpisy. Mogą one dotyczyć osób, sytuacji , wydarzeń. Takie obrażanie nazywamy **hejtem.** Osoba, która publikuje agresywne, obraźliwe komentarze ,pozbawione rzeczowej argumentacji to **hejter.**

Tego rodzaju wrogie wypowiedzi mogą być postrzegane jako akty cyberprzemocy i nękania psychicznego (stalking), może w nich występować mowa nienawiści.

Cyberprzemoc

Cyberprzemoc to takie zachowania jak:

- ośmieszanie, obrażanie, straszenie, nękanie czy też poniżanie kogoś za pomocą Internetu, albo telefonu komórkowego
- podszywanie się pod kogoś w portalach społecznościowych, na blogach, wiadomościach e-mail lub komunikatorach
- włamanie się na czyjeś konto (np. pocztowe, w portalu społecznościowym, konto komunikatora)
- publikowanie oraz rozsyłanie filmów, zdjęć, albo informacji, które kogoś ośmieszają
- pisanie obraźliwych komentarzy na forach, blogach, portalach społecznościowych
- Osoby, które doświadczyły cyberprzemocy czują: bezradność, wstyd, upokorzenie, strach

Jak reagować na cyberprzemoc?

Jeśli doświadczasz cyberprzemocy:

- Powiedz o tym zaufanej osobie.
- Nie kontaktuj się ze sprawcą cyberprzemocy, aby nie prowokować go do dalszych działań.
- Zachowaj dowody : nie kasuj smsów, e-maili, rozmów na komunikatorach. Zrób zrzut ekranu.

Jeśli jesteś świadkiem cyberprzemocy:

- Nie przesyłaj dalej ośmieszających wiadomości.
- Pomóż pokrzywdzonej osobie poprzez rozmowę na ten temat.
- Zaproponuj pokrzywdzonej osobie kontakt z profesjonalną placówką np..Helpline.org.pl

Wirusy

Konieczne jest korzystanie z oprogramowania antywirusowego. Jeszcze niedawno antywirusy były jedynie zalecane do użytku. Dziś komputer bez jakiegokolwiek zabezpieczenia jest praktycznie nie do użytku. Ochrona przed zagrożeniami jest już zdecydowanie obowiązkowa dla każdego. Na rynku dostępne są dziesiątki różnych programów, zarówno płatnych jak i darmowych.

Fałszywe profile- kradzież tożsamości, wyłudzanie informacji

Na forach społecznościowych, cyberprzestępcy podszywają się pod inne osoby i naciągają w wiadomościach na pieniądze lub wykonują inne krzywdzące czynności. Takie sfałszowane profile można jednak stosunkowo **łatwo rozpoznać po kilku typowych cechach**: najczęściej nie są zbyt długo aktywne, a aktualizacje statusu są ekstremalnie rzadkie, a często wręcz nie ma ich wcale. I nawet jeśli na taki profil trafiają zdjęcia albo komentarze, to mają bardzo mało polubień. Trzeba, więc dokładnie je sprawdzić!

Źle zabezpieczone strony sklepów internetowych

Jeżeli robisz zakupy przez Internet i zakładasz konta to POD ŻADNYM POZOREM nie ustawiaj na nich hasła, z którego skorzystałeś wcześniej na innym portalu! Moduły sklepowe nie zawsze są bezpieczne – czasami przez zaniedbania twórców, a czasami przez zaniedbania samych właścicieli sklepów, którzy z danego rozwiązania korzystają. Ten punkt jest o tyle istotny, że w przypadku dużych serwisów typu Facebook.com można liczyć na bardzo rozwinięte mechanizmy zabezpieczające. W przypadku małych sklepów internetowych, należy wykazać się dużą dozą ostrożności.

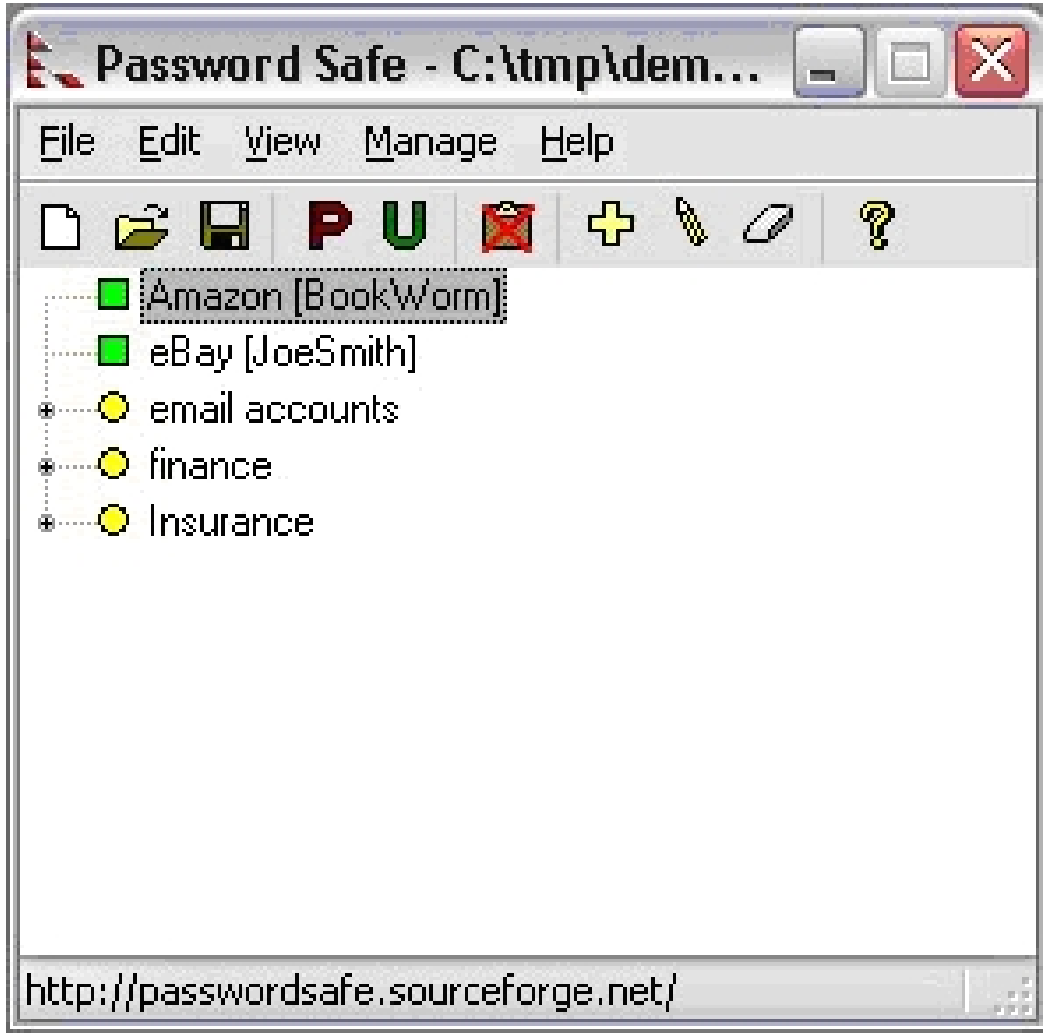
Zwiększanie bezpieczeństwa

Bezpieczeństwo w Internecie można zwiększyć.
Służą temu:

- Zabezpieczanie haseł
- Dwuetapowa weryfikacja
- Blokada rodzicielska Internetu

HASŁA

Aby zagwarantować sobie wysoki poziom bezpieczeństwa w Internecie, należy stosować trudne do złamania hasła. Bardzo wiele osób, jako hasła wybiera datę swoich urodzin, imię dziecka , znak zodiaku itp. Błąd- hasło ma być długie , skomplikowane , należy użyć znaki specjalne . Przykład MoZoVr2#WsRz7Ko**. Nie należy stosować jednego hasła do wszystkich kont jakie posiadamy.



Zabezpieczanie haseł

Większość społeczeństwa używa prostych, niekiedy takich samych haseł na swoich profilach. Są one bardzo łatwe do rozszyfrowania przez hakerów. Za pomocą specjalistycznych programów włamują się oni na konta użytkowników i kradną poufne informacje.

Najskuteczniejszym sposobem, aby uchronić się przed hackerami jest używanie menedżera haseł np. Last Pass. Tworzy on, zapamiętuje i zarządza naszymi hasłami na stronach internetowych oraz w aplikacjach, pomiędzy wszystkimi urządzeniami.

Użytkownik musi zatem pamiętać tylko jedno, główne hasło do Last Pass – całą resztą usługa zajmie się sama.

Jeżeli jednak nie skorzystasz z tych usług to pamiętaj, aby nie ustawiać tych samych haseł do wielu kont np. poczty, Facebooka i Allegro. Wyciek hasła z jednego miejsca jeszcze nie oznacza utaty wszystkich danych, ale jeżeli tego samego hasła użyłeś w kilku serwisach w najlepszym wypadku możesz utracić kontrolę nad swoją tożsamością w sieci.

Dwuetapowa weryfikacja

Aby jeszcze lepiej zabezpieczyć konta warto włączyć weryfikacje dwuetapową.

- Weryfikacja dwuetapowa to dodatkowe zabezpieczenie konta. Po jej skonfigurowaniu będziesz logować się na swoje konto w dwóch etapach za pomocą dwóch składników:
- czegoś, co znasz (Twojego hasła);
- czegoś, co masz (Twojego telefonu lub klucza bezpieczeństwa).

Można włączyć ją w ustawieniach poszczególnych portali.

Blokada rodzicielska Internetu

- filtruje strony internetowe pod kątem treści nieodpowiednich dla najmłodszych (np. pornograficzne, przemocowe),
- nadzoruje uruchamiane aplikacje - pozwala na weryfikowanie częstotliwości i czasu z nich korzystania,
- blokuje opcje pobierania programów i aplikacji- próba zainstalowania czegoś musi być autoryzowana przez rodzica,
- chroni bezpieczeństwo plików - nic przypadkowo nie zostanie skasowane,
- uniemożliwia ściągniecie zawirusowanego pliku,
- uniemożliwia kontakty dziecka z osobami, z którymi do czynienia mieć nie powinno,
- pozwala na kontrolę czasu spędzanego w sieci - można skorzystać z opcji konfigurowania limitów czasu korzystania z urządzenia.

Źródła

- https://www.edukacjakonsumencka.pl
- https://www.spidersweb.pl
- http://www.edziecko.pl/rodzice
- https://www.poradykomputerowe.pl
- http://www.zsonr1.gliwice.pl
- https://image.slidesharecdn.com

opracowanie:

Krystyna Woźniak Agnieszka Lewicka