PISMO UCZNIÓW ZSZ W GOSTYNIU

SKRZAT

WYDANIE SPECJALNE

NO
81

Kwiecień 2014

Miesięcznik nieregularny

DZIEŃ BEZPIECZNEGO INTERNETU 2014

11 LUTEGO

ins@fe

www.dbi.pl

NASK

FUNDACJA DZIECI NICZYJE

s@ferinternet.pl

Główny Partner Fundacja Orange

Witajcie…

… w specjalnym numerze Schizola. W całości jest on poświęcony bezpiecznemu korzystaniu z Internetu, komputera czy telefonu komórkowego. Ma to związek z tegorocznymi obchodami Dnia Bezpiecznego Internetu w naszej szkole.

Dzień Bezpiecznego Internetu (DBI) obchodzony jest z inicjatywy Komisji Europejskiej od 2004 roku i ma na celu inicjowanie i propagowanie działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych. W Polsce Dzień Bezpiecznego Internetu od 2005 roku organizowany jest przez Fundację Dzieci Niczyje oraz Naukową i Akademicką Sieć Komputerową (NASK) – realizatorów unijnego programu Safer Internet. Głównym partnerem wydarzenia jest Fundacja Orange.

DBI ma na celu przede wszystkim inicjowanie i propagowanie działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych, zaznajomienie rodziców, nauczycieli i wychowawców z problematyką bezpieczeństwa dzieci w Internecie oraz nagłośnienie tematyki dotyczącej bezpieczeństwa online.

Hasło tegorocznych obchodów „Razem tworzymy lepszy Internet" ("Let's create a better Internet together") ma zwrócić uwagę na fakt, że każdy internauta może przyczynić się do tego, że Internet będzie miejscem bezpiecznym i pozytywnym.

W szkole podjęto szereg działań, które miały nam wszystkim to uświadomić. Odbyły się spotkania z policjantem na temat cyberprzemocy, spotkania z psychologiem dotyczące samotności w sieci, na godzinach wychowawczych rozmawialiście o zagrożeniach wynikających z nadużywania telefonów komórkowych i komputera/ Internetu. Uczniowie technikum informatycznego wykonali filmy poświęcone tym tematom, mogliście wiele dowiedzieć się z lekcji z pedagogiem czy gazetek, które powstały na temat. Wszystko po to, by uzmysłowić sobie, **że każdy z nas ponosi odpowiedzialność za to, co robi w Sieci i w jaki sposób z niej korzysta**.

Mam nadzieję, że zawarte w wydaniu specjalnym Schizola informacje przydadzą się w Waszym codziennym życiu.

Artykuły w Schizolu zostały zaczerpnięte ze strony: helpline.org.pl i www.saferininternet.pl Chcecie wiedzieć więcej - zachęcam, by do nich zajrzeć.

Uśmiecham się do Was
Katarzyna Kozłowska - pedagog

Bezpieczny komputer

Poniżej dowiesz się, w jaki sposób chronić swój komputer przed niebezpiecznymi programami i osobami w sieci.
Nie zapominaj, że podczas korzystania z Internetu możesz, a wręcz musisz dbać o bezpieczeństwo komputera. W ten sposób ochronisz nie tylko zawarte na nim informacje, ale także siebie i innych.
By komputer naprawdę był chroniony, pamiętaj, aby uaktualniać przeznaczone do tego programy.

O bezpieczeństwo swojego komputera warto zadbać od samego początku, czyli od momentu wyboru komputera oraz jego głównego oprogramowania, czyli systemu operacyjnego.

Nowy komputer może być wyposażony w system bądź też system musimy zakupić oddzielnie. Zakupiony system należy zainstalować i odpowiednio zmienić ustawienia, czyli skonfigurować. Konfiguracja służy między innymi temu, by móc korzystać z niego w bezpieczny sposób.

Jak zainstalować system i odpowiednio zmienić jego ustawienia, aby bezpiecznie korzystać z komputera?

Instalacja systemu jest dosyć skomplikowana i bardzo ważna, jeśli chodzi o późniejsze korzystanie z komputera. Dlatego najlepiej poproś o pomoc swoich rodziców lub inną osobę dorosłą, która wie, jak zainstalować system.

Instalując system, warto pamiętać o następujących zasadach:

1. Po pierwsze, instaluj TYLKO legalne oprogramowanie. Nie tylko dlatego, że wersje „pirackie" są zabronione – tego typu programy mogą również zawierać „zaszyte" złośliwe oprogramowanie. Instaluj najnowsze, aktualne wersje programów – większość programu pozwala na sprawdzenie, czy korzystasz z najnowszej wersji.

2. Jeśli instalujesz system operacyjny, rób to tylko wtedy, gdy komputer nie jest podłączony do Internetu. Tę czynność wykonasz dopiero, gdy ustawisz i sprawdzisz wszystkie zabezpieczenia.

3. Oprócz systemu i zabezpieczeń komputera ważne jest odpowiednie ustawienie i zabezpieczenie połączenia z Internetem. Jeśli łączysz się bezprzewodowo, trzeba również zabezpieczyć router, czyli urządzenie, dzięki któremu możesz korzystać z sieci bezprzewodowej.

4. Włącz automatyczne aktualizacje używanych programów, w szczególności systemu operacyjnego (w systemie Windows w menu Start >> Ustawienia >> Panel sterowania >> Aktualizacje automatyczne).

5. Wyłącz usługi, z których nie korzystasz z sieci, np., jeśli Twój komputer nie jest połączony z innymi komputerami w domu możesz wyłączyć „Współużytkowanie plików i drukarek w sieci".

6. Upewnij się, czy masz włączony program antywirusowy oraz zaporę sieciową (przynajmniej tę wbudowaną w system Windows).

7. Sprawdź ustawienia przeglądarki internetowej**.** Jeśli masz przeglądarkę internetową Internet Explorer, upewnij się, czy w jej opcjach nie jest ustawiony najniższy poziom bezpieczeństwa lub ochrony prywatności.

Dodatkowe zabezpieczenia w komputerze:
Pewna ilość zabezpieczeń wbudowana jest bezpośrednio w system operacyjny. Warto jednak skorzystać z dostępnych w sieci bezpłatnych programów. Bezpłatne nie oznacza złe – firmy je tworzące dzięki informacjom uzyskiwanym z Twojego komputera mogą doskonalić wersje płatne swoich programów, przeznaczone dla firm.

- **Zapora sieciowa (firewall)**
  Zapora sieciowa (tzw. firewall, ściana ogniowa) to jeden z najważniejszych elementów chroniących Twój komputer podczas korzystania z Internetu. Zapobiega atakom, rozpoznaje większość prób włamań i blokuje je.

- **Programy antywirusowe**
  Zabezpieczają komputer w sieci przed wirusami. Uwaga! Są skuteczne tylko wtedy, gdy posiadają aktualną bazę wirusów, czyli są na bieżąco aktualizowane, co zazwyczaj dzieje się automatycznie.

Wszystkie zabezpieczenia w jednym

Dla ochrony komputerów domowych istnieją także tzw. pakiety bezpieczeństwa. To programy, łączące oprogramowanie antywirusowe, zaporę ogniową, oprogramowanie antyspamowe, antyszpiegowskie, itd. Tego typu kompleksowe rozwiązania zazwyczaj są płatne. Kompleksowe rozwiązanie e-bezpieczeństwo oferuje swoim Klientom Orange Polska, inne przykłady to m. in. G DATA Internet Security TotalCare, Symantec Norton 360, McAfee Total Protection. Można też zajrzeć na stronę Microsoft OneCare (po angielsku). Wspólnie z rodzicami możecie zastanowić się, czy decydujecie się na używanie często darmowych osobnych programów czy też kompleksowego, płatnego pakietu zabezpieczeń.

Jak bezpiecznie używać komputera podłączonego do Internetu?

- Zanim podłączysz komputer do Internetu, sprawdź, czy masz włączoną zaporę sieciową i program antywirusowy lub poproś o to rodziców bądź zaufaną osobę dorosłą.

- **Wspólnie z rodzicami regularnie aktualizuj system** operacyjny i pozostałe oprogramowanie, którego używasz w komputerze. **Ważne jest też, by sprawdzać wraz z rodzicami, czy ustawienia bezpieczeństwa tych programów są odpowiednie.**

Aktualizacja programów jest bardzo ważna, bowiem ich producenci stale umieszczają w sieci pewne poprawki, łatające wykryte luki bezpieczeństwa bądź po prostu powodujące, że program lepiej i szybciej działa. Aktualizacje należy pobrać z sieci i zainstalować. Zazwyczaj dzieje się to automatycznie – program sam je wykrywa, ściąga i instaluje. Zdarza się jednak, że program nie jest ustawiony tak, aby automatycznie ściągać

aktualizację. W takiej sytuacji należy to zmienić w ustawieniach programu lub regularnie pobierać aktualizacje poprzez kliknięcie w menu programu odpowiedniej opcji.

- **Pamiętaj, by program antywirusowy był zawsze aktualny i stale włączony.**
- **Regularnie sprawdzaj stan zabezpieczeń swojego komputera oraz reaguj na wszelkie pojawiające się zagrożenia**. Nie musisz wszystkiego robić sam/a. Poproś rodziców o pomoc w ustawieniu regularnego skanowania komputera programem antywirusowym i w ustawieniu zapory sieciowej. Regularnie sprawdzajcie stan zabezpieczeń (np. system Windows możesz sprawdzić oprogramowaniem Microsoft Baseline Security Analyser).
- **Zachowaj szczególną ostrożność podczas korzystania z Internetu**. Nawet najlepszy program nie jest w stanie zapewnić Twojemu komputerowi pełnej ochrony, jeśli odwiedzasz nieznane strony, uruchamiasz ściągnięte z nich programy lub otwierasz załączniki z e-maili od nieznanych osób. W takich przypadkach najważniejsza jest Twoja świadomość, czyli ostrożne zachowanie w sieci.
- **Stosuj bezpieczne hasła dostępu.**
- **Pamiętaj! Nie możesz mieć stuprocentowej pewności, że na Twoim komputerze nie zostanie zainstalowane oprogramowanie szpiegujące. Każdy może stać się ofiarą oszustwa sieciowego. Szansa na to jest znacznie mniejsza, jeśli dbasz o bezpieczeństwo swojego komputera.**

Ochrona przed złośliwym oprogramowaniem
Zapobieganie infekcji

Czym jest złośliwe oprogramowanie (m.in. wirusy, trojany, itd.)? Jak najlepiej się przed nim bronić?
Złośliwe programy przenoszą się między komputerami – czasem mogą to zrobić dzięki Twojej nieuwadze, innym razem wykorzystają „dziurę" w jednym z Twoich programów, by zainstalować się bez Twojej wiedzy. Taki program może usunąć przydatne informacje z Twojego komputera, wysyłać bez Twojej wiedzy pocztę elektroniczną, przekazać kontrolę nad Twoim komputerem przestępcy, a nawet go uszkodzić.
Czy wiesz, jak złośliwe oprogramowanie może się przemieszczać? Często przesyłane jest przez załączniki w wiadomościach mailowych, linki w komunikatorach internetowych (Gadu-Gadu, Facebook Messenger), śmieszne kartki, zabawne pliki wideo.
Jak ochronić się przed złośliwymi programami?

- **Bardzo ważne jest, aby dbać przez cały czas o odpowiednią ochronę swojego komputera.** Do tego służą **program antywirusowy** (który może usuwać złośliwe programy, ostrzegać przed fałszywymi witrynami czy uprzedzać przed stronami zawierającym złośliwy kod) oraz **firewall** (działający jak zapora niedopuszczająca szkodliwych elementów i ataków z zewnątrz). Zarówno program antywirusowy, jak i firewall możesz zainstalować sam lub poprosić o pomoc rodziców.

- **Aktualizuj programy**, z których korzystasz. Starsze wersje mogą działać bez problemu, ale błędy, które mogą zawierać, to zaproszenie wirusa do komputera. Jeśli nie wiesz, jak to zrobić, poproś o pomoc rodziców.

- **Zachowaj szczególną ostrożność, poruszając się po Internecie.** Złośliwe oprogramowanie rozprzestrzenia się także poprzez pliki, które możesz pobrać z sieci – nie tylko nielegalne, ale również te, które na pierwszy rzut oka wyglądają na legalne. Dlatego przed pobraniem pirackiego programu czy gry, warto rozważyć, czy chcesz podjąć ryzyko, zastanowić się, zanim **klikniesz w nieznany, podejrzany link** (korzystając z darmowych narzędzi UrlVoid, czy LinkScanner, możesz sprawdzić, czy pod odnośnikiem nie kryje się niebezpieczeństwo). **Bądź ostrożny, otwierając załączniki do wiadomości od nieznanych osób**, a także **potwierdzając komunikaty**, pojawiające się na ekranie monitora. Gdy zamykasz okno, które wydaje Ci się podejrzane, **nie klikaj przycisków** "**Akceptuj**", "**OK**"**,** czy nawet "**Nie**" (nie wszystko jest tym, czym się wydaje, nazwy na przyciskach nie oznaczają, że pełnią one faktycznie takie funkcje!), używaj do tego celu przycisku "**x**" w rogu okna). Nie ściągaj automatycznie rozszerzeń do przeglądarki (tzw. wtyczek - plug-in), gdy wymaga tego strona WWW, którą oglądasz.

- **Systematycznie sprawdzaj komputer na obecność wirusów,** skanując go za pomocą programu antywirusowego. Ustaw w opcjach antywirusa sprawdzanie plików, zapisywanych na komputerze – dzięki temu będziesz mieć mniejszą szansę na zainstalowanie złośliwego oprogramowania.
  O systematyczne sprawdzanie waszego komputera możesz również poprosić rodziców.

- **Używaj programów ze znanych, zaufanych źródeł.**

- **Rozmawiaj z rodzicami** zawsze, gdy zauważysz, że z komputerem dzieje się coś niepokojącego.

Leczenie infekcji

Nie zawsze wiadomo, czy nasz komputer jest zainfekowany złośliwym oprogramowaniem. To tak jak w życiu – nie od razu wiemy, że jesteśmy chorzy, ale zaczynający się katar czy kaszel są już podejrzane. ”Katarem” dla naszego komputera mogą być takie sytuacje:

- działa wolniej niż zwykle,
- przestaje reagować, często się zawiesza lub restartuje bez powodu,
- nie działają programy, które do tej pory działały,
- wyłącza się długo bądź przy wyłączaniu pojawiają się błędy,

- na portalu społecznościowym pojawiają się „Twoje” wpisy, których sobie nie przypominasz,
- nie możesz uaktualnić systemu operacyjnego,
- nie możesz uaktualnić antywirusa albo wchodzić na strony programów antywirusowych,
- Internet „pełznie”, zamiast normalnie działać,
- Twoi znajomi dostają od Ciebie maile, których nie wysłałeś (najpierw zmień hasło do programu pocztowego).

Jeśli zdarzyła Ci się któraś z rzeczy, opisanych wyżej, co wskazuje, że Twój komputer został zainfekowany, to warto:
Odłączyć komputer od sieci i zabezpieczyć przechowywane na nim informacje. Może się zdarzyć, że po wyłączeniu zainfekowanego sprzętu nie będziesz mógł go z powrotem uruchomić.
Przeskanować komputer programem antywirusowym, dzięki czemu możesz wykryć i usunąć złośliwe oprogramowanie. Jeśli nie możesz uruchomić swojego antywirusa, poproś znajomego lub rodziców, by ściągnęli z Internetu program antywirusowy, który można uruchomić z pamięci USB (tzw. pendrive’a).
Jeśli wcześniejsze działania nie rozwiążą problemu, **poproś o pomoc rodziców** lub znajomego informatyka. Jeśli on nie zdoła doprowadzić Twojego komputera do stanu sprzed infekcji – trzeba będzie od nowa zainstalować system operacyjny.

Ochrona przed rootkitami

Czym są rootkity?

Rootkit to program zmieniający działanie systemu komputerowego poprzez ukrywanie plików oraz połączeń sieciowych, odpowiadających za utrzymanie kontroli nad systemem. Przeważnie rootkity ukrywają inne złośliwe programy, np. trojany czy programy szpiegujące, by nie mogły zostać wykryte przez narzędzia zabezpieczające system. Rootkit może się dostać do komputera podobnie jak inne złośliwe programy (np. za pośrednictwem trojana).
Zasady bezpieczeństwa, które mogą znacznie zmniejszyć szansę infekcji rootkitem, są takie same, jak w przypadku wirusów. Jeśli wybieracie do swojego komputera pakiet, a nie tylko program antywirusowy, warto poradzić się rodziców bądź specjalisty, by zawierał on również narzędzia do wykrywania rootkitów.

Leczenie infekcji

- Jeśli skanowanie programem antywirusowym lub skanerem online wykryje rootkita, lecz nie usunie go, **można użyć SPECJALNEGO NARZĘDZIA ANTYROOTKITOWEGO**. Warto wtedy skorzystać z pomocy rodziców i wybrać najlepsze dla was oprogramowanie.
- **Specjalista** (zachęcamy do skorzystania z jego pomocy) **może również uruchomić komputer z płyty CD** i usunąć rootkita, zanim zostanie uruchomiony i zdoła się ukryć.

Hakerzy i włamania – ważny dla nas temat – rodzaje ataków oraz zagrożenia związane z atakami i włamaniami a także informacja hakerzy/krakerzy

Zakupy w Internecie, gazety, filmy, nawet – o zgrozo – dzienniki szkolne :) - to wszystko coraz częściej z realnego świata przenosi się do sieci. Niestety, tam gdzie dzieje się dużo, trafiają również źli ludzie. Dlatego coraz większe jest ryzyko, że ktoś włamie się na nasz komputer, nasze konto (np. na Facebooku) albo ukradnie dane, których nie chcemy ujawnić.

By przestępcy mogli przejąć kontrolę nad Twoim komputerem, muszą na nim zainstalować niewielki, złośliwy program, tzw. malware. Najczęściej jednak robisz to nieświadomie Ty, gdy klikniesz w link w dziwnym mailu, który niespodziewanie do Ciebie przyszedł (często od kogoś znajomego), w coś, co „polubił" Twój znajomy na Facebooku lub przysłał Ci na czacie bądź GG. **To, że dziwny link dostałeś/aś od znajomej osoby, nie musi oznaczać, że to ona go wysłała** – przestępcy mogli przejąć również jej komputer.

Kiedyś złośliwe oprogramowanie można było „schować" tylko w tzw. plikach wykonywalnych (np. exe) – teraz przestępcy potrafią je ukryć w niewyglądających podejrzanie zdjęciach (jpg), plikach tekstowych Word (doc), arkuszach Excel (xls), czy plikach pdf. Takie pliki wykorzystują luki w zabezpieczeniach programów (tzw. podatności) i instalują malware bez Twojej wiedzy.

Jak jeszcze przestępcy mogą zainfekować Twój komputer?

- Gdy otwierasz plik, np. ściągnięty z Internetu, przysłany pocztą (przede wszystkim w przypadku, gdy nie spodziewałeś/aś się maila od nadawcy!).
- Po wejściu na podejrzaną stronę. Np. taką z pirackimi filmami/grami czy zdjęciami/filmami „dla dorosłych", ale też, gdy klikniesz w link, przysłany w spamie.
- Kiedy nie robisz nic podejrzanego. Serio. Przestępcy mogą przejąć niebudzącą podejrzeń stronę i nic na niej na pierwszy rzut oka nie zmieniać. Po wejściu na taką stronę „schowane" tam złośliwe oprogramowanie korzysta np. z luk w przeglądarce internetowej.

Czym możesz zarazić swój komputer? Złośliwe oprogramowanie często nazywamy ogólnie po prostu wirusami, tak naprawdę jest jednak kilka rodzajów mniej lub bardziej niebezpiecznego malware'u. Najgroźniejsze złośliwe programy to tzw. „hybrydy", będące skrzyżowaniem np. trojana i keyloggera. Więcej informacji o rodzajach złośliwych programów znajdziesz w Słowniku.

Złośliwe oprogramowanie może np.:

- wyświetlać na ekranie różne (także złośliwe) napisy,
- uszkadzać albo kasować dane,
- spowolniać pracę komputera (wtedy, gdy łączy się z serwerem sterującym *botnetu*),
- wyłączać niektóre programy (np. antywirusowe),
- bez Twojej wiedzy rozsyłać *spam* albo ukryć na Twoim komputerze np. podrobioną stronę banku,
- ukraść trzymane na komputerze hasła, dane osobowe i numery kart kredytowych.

Po czym poznać, że Twój komputer może być właśnie atakowany albo kontrolują go przestępcy?

- Długo się wyłącza lub pokazuje jakieś dziwne komunikaty.
- Na portalu społecznościowym pojawiają się „Twoje" wpisy, których sobie nie przypominasz.
- System operacyjny (np. Windows) albo program antywirusowy nie chcą się uaktualnić.
- Internet działa bardzo powoli.
- Twoi znajomi dostają od Ciebie maile, których nie wysyłałeś/łaś.

Te sytuacje nie muszą oznaczać, że dzieje się coś złego, ale warto sprawdzić komputer programem antywirusowym (jeśli to antywirus nie działa, trzeba ściągnąć go z internetu na innym komputerze, nagrać na pendrive'a i wtedy podłączyć do Twojego komputera). Jeśli to problem z kontem społecznościowym albo pocztowym – **koniecznie natychmiast zmień hasło**.
Dlatego **trzeba pamiętać, by nie klikać w podejrzane linki**, niezależnie od tego, skąd i w jaki sposób przyszły. Zawsze możesz zadzwonić do znajomego i spytać, czy aby na pewno przysłał Ci dziwnie wyglądającego maila albo „polubił" coś dziwnego. Jeśli pojawi Ci się prośba o ściągnięcie aktualizacji jakiegoś programu, sprawdź, czy na pewno link prowadzi na dobrą stronę! Pamiętaj jednak, że to co widzisz, może być mylące – najlepiej najechać kursorem na link (bez klikania)
i jeśli adres, który pojawi się na dole przeglądarki, różni się od tego, który jest w treści strony, ktoś usiłuję Cię oszukać.
Zawsze możesz też poprosić o pomoc rodziców lub znajomego informatyka.
Aha, i wbrew temu, co mówią w filmach, na Twój komputer wcale nie włamią się hackerzy. *Hacker* to człowiek, który wyszukuje błędy w zabezpieczeniach w dobrej wierze, by można je było „załatać", zanim stanie się coś złego. Złym człowiekiem, które te błędy wykorzystuje, jest *cracker*.
I niekoniecznie pisze na klawiaturze szybciej niż zawodowa maszynistka – po prostu według scenarzystów z Hollywood tak wygląda się bardziej profesjonalnie :).

Spam

W USA Spam znają już od 1937, a na dodatek można go... kupić w sklepie. Niechciana poczta elektroniczna, bo to o niej będzie dalej, przejęła bowiem tę nazwę od mielonki w puszce. W latach 80., w czasach prehistorii sieci, gdy korzystano z BBSów i grano w MUDy, źli ludzie, by „zagłuszyć" konwersację, pisali na ekranie słowo Spam do momentu aż cała pozostała treść przewijała się poza ekran.
Dzisiejszy Spam to niechciane e-maile, zazwyczaj takie,
w których jesteśmy namawiani do bezpośredniego kupna leków dostępnych tylko na receptę albo do kliknięcia w link. Przy lekach tracimy pieniądze i ryzykujemy zdrowie (bo nie wiadomo, co taka „apteka" nam przyśle), zaś w drugim przypadku najpewniej skończy się to zainstalowaniem na komputerze złośliwego oprogramowania.

Spam przynosi ludziom, którzy go wysyłają, olbrzymie dochody, dlatego średnio 9 na 10 wysyłanych na świecie maili to właśnie spam. Dostawcy Internetu radzą sobie z nim coraz lepiej, zarówno blokując możliwość wysyłania takich maili
z komputerów, które kontrolują przestępcy (blokada portu 25 w Orange Polska), jak i zatrzymując podejrzane maile przychodzące.
Skąd przestępcy mają adresy, na które wysyłają spam?
M.in. dzięki specjalnym programom, szukającym w sieci
e-maili wpisanych na przykład na stronie WWW, wykradając je ze słabo zabezpieczonych forów internetowych albo z listy Twoich znajomych (jeśli hasło do Twojego e-maila jest na tyle słabe, żeby je złamać).

Poradnik powstał przy współpracy z TP CERT, jednostką reagowania na zagrożenia bezpieczeństwa teleinformatycznego Orange Polska (http://cert.orange.pl).

Bezpieczny Ty

Poniżej znajdziesz informacje na temat zagrożeń, które mogą dotyczyć Twojej prywatności w Internecie. Tutaj dowiesz się również, jak można im zapobiegać.

- **Zagrożenia dla Twojej prywatności w sieci**

Choć Internet jest nazywany rzeczywistością wirtualną, czające się w nim zagrożenia są jak najbardziej prawdziwe. Dlatego, korzystając z serwisów społecznościowych (np. Facebooka) czy nawet wysyłając i odpowiadając na maile, trzeba bardzo uważać na to, co robimy.

Jeśli nie zmienisz początkowych ustawień prywatności Facebooka, informacje, które tam piszesz, będzie mógł przeczytać każdy. Twoje zdjęcia także nie będą ukryte. Dlatego poproś znajomego informatyka albo poszukaj w Internecie, jak zmienić te ustawienia, tak, by ważne informacje o Tobie widzieli tylko najbliżsi znajomi. Zaznacz też, by nie można Cię było otagować na zdjęciu albo w poście bez Twojej wiedzy.
Jeśli nie dbasz o prywatność na portalach społecznościowych, wystawiasz się na duże ryzyko. Twoje zdjęcia/statusy może zobaczyć ktoś, komu nie chcesz ich pokazać, na domowej imprezie będziesz miał niechcianych gości. Może się nawet zdarzyć tak, że złodziej widząc, gdzie mieszkasz i że właśnie „meldujesz" się z rodzicami, np. w kinie, będzie wiedział, że teraz ma czas, by okraść Wasze mieszkanie. **Pamiętaj – nie musisz przyjmować wszystkich zaproszeń do znajomych**, a na pewno nie od ludzi, których nie znasz – to, ilu masz znajomych na Facebooku, nie świadczy o tym, jak bardzo jesteś fajny/a...
Możesz też paść ofiarą przestępcy „sieciowego", a nie realnego. W jego ręce może trafić dostęp do Twoich kont (przede wszystkim jeśli nie ustawisz trudnego do odgadnięcia hasła) mailowych albo społecznościowych. Pół biedy jeśli tylko zablokuje do nich dostęp – gorzej, że może wysyłać maile albo publikować statusy czy zdjęcia jako Ty, a jeśli zmieni hasło, nie będziesz w stanie mu przeszkodzić.
Jeśli korzystasz z komputerów, np. w kawiarenkach internetowych, **uważaj na „hackowanie przez ramię"** – patrz, czy przypadkiem ktoś nie stoi za Twoimi plecami, kiedy wpisujesz hasło. Jeśli nie musisz, nie używaj komputerów dostępnych dla wielu osób do logowania się do serwisów, gdzie przechowujesz ważne dane. Może się okazać, że sieciowy przestępca wcześniej zainstalował na takim komputerze keylogger, więc Twój login i hasło trafią prosto do niego.

Oszustwa sieciowe

Phishing (od angielskiego fishing, czyli łowienie ryb) to jeden ze sposobów, w jaki przestępcy mogą przejąć kontrolę nad Twoim komputerem. Krótko pisaliśmy już o nim w kilku miejscach, warto jednak zastanowić się nad nim dłużej.

Wszystko rozpoczyna się od maila, który trafia na Twoją skrzynkę. Czasami wygląda dziwnie, nawet śmiesznie (teksty tłumaczone automatycznie to prawdziwa komedia!), coraz częściej jednak takie e-maile bardzo przypominają prawdziwe. Przestępcy przygotowują profesjonalne polskie tłumaczenie, dokładają do tego logo znanych i popularnych firm.

Przestępcy chcą przekonać odbiorcę maila do kliknięcia w link (a wtedy w tle, bez jego wiedzy, na komputerze zainstaluje się złośliwe oprogramowanie), poinformowania „firmy" o swoich danych wrażliwych (loginy, hasła, adresy) bądź wpisania ich na stronie internetowej.

Pamiętaj, że nie wszystko jest takim, jakim może się wydawać! **Link w mailu może wyglądać na prawdziwy, ale prowadzić do zupełnie innej strony** (często wystarczy najechać kursorem na link i zobaczyć, czy na dole w przeglądarce pojawi się taki sam adres), załączony do maila plik jpg wcale nie musi być zdjęciem (gdy je klikniesz, okaże się, że to tak naprawdę plik exe), a zwykły plik PDF albo DOC może mieć ukryty złośliwy kod.
Pamiętaj, że poważne firmy nigdy nie proszę o wysłanie im ważnych danych mailem. Jeśli masz wątpliwości, czy mail jest prawdziwy – poproś o pomoc dorosłego. Możesz też zadzwonić do firmy, na telefon podany w mailu, a wcześniej sprawdzić na jej stronie, czy numer jest prawdziwy.

Skąd przestępca tyle o Tobie wie?
Przestępcy, nie tylko internetowi, radzą sobie dobrze, m.in. dlatego że potrafią rozmawiać z ludźmi i przekonywać ich, by zrobili coś, czego tak naprawdę nie chcą. Mogą tego spróbować również z Tobą.
Przeczytaj, na co warto uważać, gdy ktoś obcy mailuje z Tobą lub rozmawia przez telefon:
Chce dać Ci za darmo coś (rzecz albo informację). **Niestety zazwyczaj nie ma nic za darmo** – za to jeśli Ty coś od kogoś dostaniesz, bardzo możliwe, że chętniej mu się czymś zrewanżujesz, np. swoim adresem e-mail, loginem, czy hasłem.
Jeśli komuś uda się Ciebie oszukać i przekonać, że np. jest policjantem albo urzędnikiem (podczas gdy tak naprawdę jest oszustem), później ciężko Ci będzie uwierzyć, że to nieprawda i możesz niechcący wprowadzić w błąd również inne osoby, np. kolegów/koleżanki.
Zdarzyło Ci się kiedyś „polubić" jakiś fanpage na Facebooku tylko dlatego, że lubili to Twoi znajomi, nie zastanawiając się nawet, co to jest? W ten sposób przestępcy gromadzą **tzw. „farmy fanów"**, takie kliknięcie może też zarazić komputer złośliwym oprogramowaniem
Z zasady chętniej pomagamy ludziom, których znamy i lubimy. Do tego stopnia, że możemy **z rozpędu** otworzyć załącznik z otrzymanego „od nich" (a tak naprawdę wysłanego przez malware) e-maila, który może okazać się wysłanym bez ich wiedzy wirusem albo kliknąć w podejrzany link.
Jeśli słyszymy, że osoba, która z nami rozmawia, jest np. z policji, nawet jeśli nie ma munduru, znaczna większość z nas jej uwierzy i chętnie pomoże. Tak jesteśmy wychowani. Dorośli, słysząc, że dzwoni ktoś z Urzędu Skarbowego, od razu biegną po potrzebne dokumenty :), nawet nie zastanawiając się, czy ten ktoś mówi prawdę! Nie wierzcie komuś, że jest kimś ważnym i trzeba słuchać jego próśb lub żądań, tylko dlatego, że tak Wam powiedział przez telefon. **To, że w podejrzanym mailu jest nazwa znanej Wam dużej firmy, nie sprawia że jest on bardziej wiarygodny.** Jeśli macie wątpliwości, pokażcie mail dorosłemu albo poproście go do telefonu.
Zdarzyło Wam się kupić coś dlatego że przeczytaliście, że promocja trwa tylko do jutra? Albo poprosić kogoś o pomoc, dlatego że sami nie zdążylibyście wykonać zadania? To oczywiście nic złego, ale **warto pamiętać, że jeśli prosi o pomoc ktoś obcy i denerwuje się, że bardzo mu się spieszy, możemy wtedy zapomnieć o zachowaniu bezpieczeństwa i zrobić coś, do czego na spokojnie nie dalibyśmy się przekonać.**

Cyberprzemoc

Cyberprzemoc to takie zachowanie, które krzywdzi emocjonalnie drugiego człowieka. Osoby, które stosują cyberprzemoc używają do tego celu Internetu albo telefonów komórkowych.

W przeciwieństwie do przemocy fizycznej, cyberprzemoc nie zostawia śladów na ciele i nie widać jej gołym okiem. Osoby, które doświadczyły cyberprzemocy, czują się zranione i bardzo przeżywają to, co je spotkało. Pojawiają się u nich nieprzyjemne myśli i uczucia, takie jak bezradność, wstyd, upokorzenie, strach, a czasem również złość.

Osoba, której przytrafiła się taka sytuacja, często ma wrażenie, że wszyscy widzieli lub mogą zobaczyć te nieprzyjemne materiały. Obawia się, że jej znajomi odwrócą się od niej i nie będzie mogła liczyć na ich wsparcie. To powoduje, że czuje się bardzo samotna w tym, co ją spotkało.

Cyberprzemoc to takie zachowania. jak:

ośmieszanie, obrażanie, straszenie, nękanie czy też poniżanie kogoś za pomocą Internetu albo telefonu komórkowego,

podszywanie się pod kogoś na portalach społecznościowych, blogach, w wiadomościach e-mail lub komunikatorach,

włamanie się na czyjeś konto (np. pocztowe, na portalu społecznościowym, konto komunikatora),

publikowanie oraz rozsyłanie filmów, zdjęć, albo informacji, które kogoś ośmieszają,

tworzenie obrażających kogoś stron internetowych lub blogów,

pisanie obraźliwych komentarzy na forach, blogach, portalach społecznościowych.

Osoby, które doświadczają cyberprzemocy ze strony innych, często czują się osamotnione i cierpią.

Pamiętaj! Nie jesteś sam/a!

Jeśli doświadczasz cyberprzemocy:

*powiedz o tym zaufanej osobie dorosłej - z jej pomocą będzie Ci łatwiej poradzić sobie z tą sytuacją,

*postaraj się nie kontaktować ze sprawcą cyberprzemocy i nie odpowiadać na jego zaczepki. Dzięki temu unikniesz prowokowania go do dalszych działań,

*zachowaj wszystkie dowody cyberprzemocy - nie kasuj smsów, e-maili, rozmów na czatach lub komunikatorach,

* jeśli ktoś dokucza Ci na jakiejś stronie WWW, zrób jej screen,

- aby zachować to, co widzisz na ekranie, wciśnij klawisz "Print Screen" (Prt Sc), a następnie otwórz program tekstowy (np. Word) lub graficzny (np. Paint) i wklej tam screen, naciskając jednocześnie klawisze "Ctrl" i "V". Pamiętaj, aby zapisać plik!

*skontaktuj się z bezpłatnym numerem 800 100 100, wyślij wiadomość e-mail na adres helpline@helpline.org.pl lub porozmawiaj na czacie z poziomu podanej strony.

Jeśli jesteś świadkiem cyberprzemocy:

*nie przesyłaj dalej ośmieszających wiadomości,

*pomóż pokrzywdzonej osobie poprzez poinformowanie kogoś dorosłego o jej sytuacji,

*zaproponuj pokrzywdzonej osobie kontakt z Helpline.org.pl (lub skontaktuj się osobiście, aby dowiedzieć się, co można zrobić).

Niebezpieczne kontakty

Niebezpieczne kontakty to kolejne zagrożenie internetowe, na które warto szczególnie uważać. Chodzi tu o osoby, które kontaktując się z Tobą przez komunikator, czat, e-mail, portal społecznościowy czy inną aplikację, mogą mieć wobec Ciebie złe intencje.
W Internecie, tak jak w życiu, spotykamy zarówno dobrych, jak i złych ludzi. Poznając osobę w sieci, zazwyczaj nie posiadamy wielu informacji na jej temat. Zdarza się, że nie jest tym, za kogo się podaje i próbuje wydobyć od Ciebie poufne informacje, intymne zdjęcia lub przekonać cię do zrobienia czegoś, co będzie niezgodne z prawem lub niebezpieczne dla Twojego zdrowia i życia. Może również dążyć do tego, aby wyłudzić od Ciebie pieniądze lub cenne rzeczy.
W przypadku znajomości z sieci warto zachować szczególną ostrożność.
Nigdy nie wiadomo, kto jest po drugiej stronie.
Jeśli podejrzewasz, że osoba, z którą nawiązałeś/aś kontakt w sieci ma wobec Ciebie złe zamiary, postaraj się:

- Zachować korespondencję z tą osobą - w historii komunikatora, e-mailach, sms'ach itp.
- Spróbuj przypomnieć sobie wszystkie informacje, które posiadasz na temat tej osoby.
- Spróbuj porozmawiać o tym z rodzicami czy inną zaufaną osobą dorosłą. Rodzice lub prawni opiekunowie mogą podjąć działania, które zapewnią Ci bezpieczeństwo.

Pamiętaj!
Masz prawo odmówić rozmów na tematy intymne i każdy powinien to uszanować.
Masz prawo przerwać każdy kontakt, który Cię niepokoi.
Masz prawo powiedzieć o wszystkim rodzicom/opiekunom prawnym.
Masz prawo zgłosić administratorowi portalu każdą sytuację, która nie jest zgodna z jego regulaminem.

Kilka wskazówek, jak bezpiecznie kontaktować się z innymi:
Staraj się spotykać przede wszystkim z osobami, które poznałeś/aś w świecie realnym.
Nie podawaj nieznajomym swoich danych osobowych, takich jak numer telefonu i adres, numer komunikatora, e-mail.
Posługuj się Nickiem, nie podawaj prawdziwego imienia i nazwiska.
Nie rozmawiaj z osobami poznanymi w sieci na tematy związane ze sferą seksualną człowieka.
Nie opowiadaj nieznajomym o Twoich prywatnych sprawach ani o Twojej rodzinie.
Bądź ostrożny z wysyłaniem zdjęć, nigdy nie wiesz, gdzie mogą później trafić!

Nieuprawniony dostęp

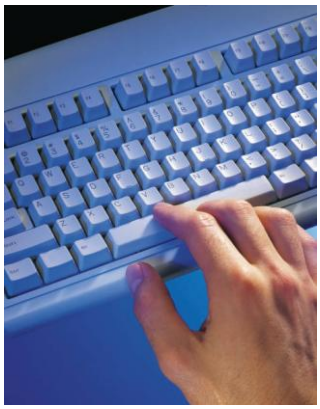
Zdarza się, że ktoś bez naszej wiedzy i zgody próbuje uzyskać dostęp do naszego komputera, konta, profilu czy bloga. Często chce w ten sposób uzyskać i przejąć informacje, które publikujemy lub przechowujemy.

Kradzież danych polega na wyciąganiu pewnych informacji (m.in. danych osobowych) od konkretnej osoby, przez osoby niepowołane (które nie mają na to pozwolenia).

Każdy Polak ma prawo do ochrony danych osobowych w myśl Ustawy o Ochronie danych osobowych z dnia 29 sierpnia 1997 roku.

Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Daną osobową będzie więc każda informacja, pozwalająca na ustalenie tożsamości osoby, nawet pośrednio, poprzez inne posiadane informacje. Daną osobową będzie mógł stanowić np.: **adres IP komputera, zdjęcie, adres email (w szczególności jeśli składa się z imienia i nazwiska)**, jeśli przy ich pomocy możemy ustalić, kim jest dana osoba.

Skradzione dane wywołują wiele zamieszania. Problemem może być wtedy nie tylko spam (niezamawiana poczta - np. reklama kosiarek do trawy), ale także ktoś może się pod nas podszywać. Udając nas, taka osoba może np. dokonywać zakupów na nasze konto.



Kiedy szczególnie narażamy się na nieuprawniony dostęp?

Poprzez korzystanie z programów niewiadomego pochodzenia. Takie programy mogą zawierać wirusy (np. uszkadzające nasz dysk, przekazujące informacje na temat tego, co robimy na swoim komputerze).

Poprzez otwieranie okienek, korzystanie linków i aplikacji z nieznanych źródeł.

Poprzez korzystanie z serwisów, portali bez odpowiednich zabezpieczeń (np. brak regulaminu, brak kontaktu z administratorem).

Poprzez podawanie hasła dostępu do naszych kont i profili innym osobom.

Poprzez dzielenie się danymi o sobie, gdy nie jest to wymagane (na różnych serwisach czy z innymi użytkownikami sieci).

Jak się chronić?

Jest kilka zasad bezpieczeństwa, których należy przestrzegać:

NIE PODAWAJ nikomu danych (chyba, że są wymagane przy rejestracji - wtedy tylko w sprawdzonych serwisach publicznych).

Gdy ktoś wypytuje Cię o Twoje dane - **NIE ODPOWIADAJ,** najlepiej skończyć taką rozmowę.

Jeżeli nie musisz, **NIE UMIESZCZAJ** ważnych danych na komputerze podłączonym do sieci.

BĄDŹ OSTROŻNA/Y w nowych miejscach w sieci - nie wiadomo, jak działają – sprawdź, jaki jest regulamin miejsca oraz czy możliwy jest kontakt z administracją.

SPRAWDŹ ZABEZPIECZENIA podczas zakupów w sieci, dbaj cały czas o odpowiednią ochronę swojego komputera.

ZAINSTALUJ PROGRAM ANTYWIRUSOWY i WŁĄCZ FIREWALL (działający jak zapora nie dopuszczająca szkodliwych elementów).

AKTUALIZUJ PROGRAMY, z których korzystasz.

BĄDŹ CZUJNA/Y- niezależnie od użytego zabezpieczenia nie mamy pewności, czy będzie ono wystarczające.

Włamania zdarzają się również na telefony komórkowe. Telefony komórkowe nowej generacji mają funkcje zbliżone do komputerów, przez co są narażone na działania wirtualnych przestępców. Zdarza się, że pobierając z Internetu na telefon grę lub aplikację niewiadomego pochodzenia, możemy wraz z nią ściągnąć wirusa. Taki wirus może zniszczyć cały system operacyjny telefonu oraz doprowadzić do utraty wszystkich danych i kontaktów, które mieliśmy w nim zapisane.

Jak się zabezpieczyć?

Włączaj usługę bluetooth i WIFI tylko wtedy, gdy z niej korzystasz.
Nie akceptuj propozycji połączenia z nieznanymi urządzeniami.
Nie pobieraj aplikacji i gier z nieznanych źródeł.
Zawsze czytaj regulaminy aplikacji i gier, które zamierzasz pobrać.

Co można zrobić w przypadku kradzieży?

W przypadku **kradzieży tożsamości** w Internecie, należy przede wszystkim zwrócić się do prowadzących serwisy, w których znajdują się przejęte przez hakera konta. Wykorzystaj e-mail i szybko **skontaktuj się z administratorami** - opisz dokładnie sytuację, tak aby uwiarygodnić problem i poproś o zablokowanie kont tak szybko, jak to możliwe. Dzięki temu nie stracisz swojej reputacji przez np. spamowe wpisy na forach spod Twojego nicka.
Jeśli nie możesz znaleźć adresu administratora strony, skontaktuj się z Helpline.org.pl i opowiedz o swoim problemie. Wątpliwości konsultować można ze specjalistami z Helpline.org.pl - www.helpline.org.pl, helpline@helpline.org.pl, tel. 800-100-100.
Poza tym należy **zmienić wszystkie hasła i loginy do serwisów internetowych, z których korzystasz**, tak żeby nie było możliwe logowanie przy użyciu starych danych. Zrób to nawet, jeśli te konta wydają się być nienaruszone - być może ktoś zechce skorzystać z nich w przyszłości.
Także sytuacja, w której korzystasz z jednego hasła do większej grupy witryn, jest niebezpieczna - **zmień to hasło** czym prędzej (a najlepiej stwórz kilka różnych).
I wreszcie trzeba też sprawdzić, czy i jakie transakcje zostały zawarte w serwisach aukcyjnych czy sklepach internetowych, gdzie mamy konta. Wszelkie „dodatkowe" zakupy czym prędzej anuluj oraz skontaktuj się ze sprzedawcami, wyjaśniając problem.
W sytuacji, gdy nie będziesz wiedział/ła, jak to zrobić bądź będą działy się rzeczy, które Ciebie niepokoją, zachęcamy do kontaktu z Helpline. Helpine.org pl pomaga w sytuacjach, gdy

przydarzy Wam się coś niebezpiecznego w Internecie lub przy użyciu telefonu komórkowego. Jeżeli skradzione zostały dane związane z kontem bankowym lub kartą kredytową, nie należy kontaktować się w imieniu innych osób bądź rodziców. Nie wolno korzystać z cudzych kart, jeżeli takie znajdziemy, należy opowiedzieć rodzicom bądź zaufanej osobie dorosłej o całej sytuacji.

Zgłoszenie przestępstwa

Jeśli skradziono Ci wyłącznie dane o niskiej wartości, np. login do forum dyskusyjnego, wtedy Twoje działania powinny się raczej ograniczyć do zabezpieczenia konta oraz komputera przed kolejnymi atakami.

Jeżeli jednak skradzione zostały dane do Twojej karty kredytowej lub też wykonano jakieś zakupy na Twoje konto - wtedy należy bezzwłocznie **skontaktować się z policją.**

Jeżeli korzystałeś z karty kredytowej rodziców lub ktoś wykonał zakupy na Twoje konto, ktoś włamał sie na Twoje konto, profil, blog, ktoś podszywa się pod ciebie w celu ośmieszenia, padłeś ofiarą nękania, zastraszania i gróźb w Internecie lub za pośrednictwem telefonów komórkowych, jest to wykroczenie i możesz zgłosić je na policję. Jeżeli masz mniej niż 18 lat w takiej sytuacji zawiadomienie na policję lub do prokuratury składają w Twoim imieniu osoby dorosłe: rodzice lub opiekunowie prawni.

Co można zrobić, jeśli ktoś przejął dostęp do konta?

1. Należy przede wszystkim niezwłocznie **skontaktować się z administracją** poprzez formularz kontaktowy z adresu e-mail, który został użyty podczas rejestracji. Gdy dostęp do poczty elektronicznej również został przejęty, kontakt ten można uzyskać pisząc z jakiegokolwiek adresu (domownika, alternatywnego konta pocztowego). Ważne, żeby zgłosiła to osoba, której dokonano kradzieży konta osobiście, a nie poprzez osoby trzecie!

W momencie powiadomienia administracji o zaistniałym incydencie należy przede wszystkim podać: login, link do profilu, adres e-mail użyty podczas rejestracji (a także informację, czy posiadasz do niego dostęp), datę urodzenia, przybliżoną lub rzeczywistą datę utracenia dostępu do profilu, nazwę dostawcy internetowego, a także personalia osoby, którą podejrzewasz o nieuprawnione korzystanie z Twojego konta.

2. Ważne, by **zmienić hasło.**

3. W sytuacji gdy nie będziecie wiedzieli, jak to zrobić bądź będą działy się rzeczy, które Was niepokoją, zachęcamy Was do kontaktu z Helpline.

4. Niezależnie od zgłoszenia włamania poprzez formularz kontaktowy, masz możliwość **powiadomienia o tym policji.** Należy wtedy podać dane personalne, login i link do profilu. Pomocnym byłoby wskazanie, który adres e-mail ma być przypisany do profilu (w przypadku braku możliwości odzyskania dostępu do pierwotnego adresu). Sprawa włamania leży jak najbardziej w kompetencjach policji, gdyż **bezprawne przejęcie kontroli nad kontem jest przestępstwem (kodeks karny art.267 i 268a)!!!.** Wyłącznie rodzice lub opiekunowie prawni mogą zgłosić przestępstwo w Waszym imieniu.

Zadbaj o bezpieczeństwo konta!

Bezpieczeństwo konta należy traktować bardzo poważnie. Aby Twój komputer i konto pozostały bezpieczne, zalecamy regularne wykonywanie następujących czynności:

Sprawdzaj, czy na komputerze nie ma wirusów i niebezpiecznych programów. Uruchamiaj skanowanie swojego komputera, korzystając ze sprawdzonego oprogramowania antywirusowego. Jeśli skanowanie wykryje podejrzane programy lub aplikacje, usuń je natychmiast.

Regularnie aktualizuj opcje odzyskiwania konta. Pamiętaj o aktualizowaniu opcji odzyskiwania konta, aby były one stale aktualne.

Zmieniaj swoje hasło przynajmniej dwa razy w roku. Wybieraj hasła zawierające kombinację cyfr, znaków i liter o różnej wielkości, co pozwoli zwiększyć bezpieczeństwo Twojego konta.

Wykonuj regularnie aktualizacje systemu operacyjnego i przeglądarki. Niezależnie od tego, czy używasz systemu Windows, czy Mac OS, zalecamy włączenie ustawienia automatycznej aktualizacji i aktualizowanie systemu po otrzymaniu odpowiedniego powiadomienia. Aby sprawdzić dostępność aktualizacji w przeglądarce Internet Explorer, wybierz menu Narzędzia i kliknij polecenie Windows Update. W przeglądarce Firefox kliknij kartę Pomoc i wybierz polecenie: Sprawdź dostępność aktualizacji.

Nigdy nie używaj hasła do konta w innej witrynie. Jeśli wprowadzisz swoje hasło w zewnętrznej witrynie, a ona padnie ofiarą ataku, ktoś może podjąć próbę zalogowania się na Twoje konto przy użyciu tych samych danych.

Chroń swoje hasło. Nigdy nie wprowadzaj hasła po kliknięciu linku w wiadomości e-mail otrzymanej z niezaufanej witryny. Zawsze przechodź bezpośrednio do witryny, z której chcesz korzystać. Nigdy nie wysyłaj hasła pocztą e-mail.

Pamiętaj!!

Nigdy nie zdradzaj nikomu swojego hasła. Jeśli to jednak zrobisz, zmień je jak najszybciej.

Używaj silnego hasła i nie zapisuj go ani nie wysyłaj pocztą e-mail.

Uruchamiaj skanowanie i zmieniaj hasła natychmiast po zauważeniu jakichkolwiek zmian na koncie, które nie zostały zainicjowane przez Ciebie.

Wyloguj się po każdym użyciu komputera w miejscu publicznym. Po zakończeniu korzystania z konta kliknij link „Wyloguj się" znajdujący się w prawym górnym rogu ekranu.

Regularnie usuwaj formularze, hasła, pliki z pamięci podręcznej i pliki typu cookies (ciasteczka) w przeglądarce, szczególnie na ogólnodostępnych komputerach.

Komputerowy słownik

Język związany z obsługą komputera nie zawsze jest prosty i zrozumiały. Warto znać znaczenie pojęć, które dotyczą Twojego bezpieczeństwa podczas korzystania z sieci!

Abuse (nadużycie) - to określenie ma dwa znaczenia. Pierwsze to różne formy ataku na Twój komputer (nie tylko bezpośredni atak internetowego przestępcy, ale również otrzymywanie – i wysyłanie z Twojego komputera bez Twojej wiedzy – spamu bądź wirusów). Abuse to także jednostki w firmach, dostarczających Internet, przyjmujące zgłoszenia, dotyczące takich nadużyć. W większości przypadków można się z nimi skontaktować, wysyłając e-mail na adres abuse@nazwafirmy (w przypadku Telekomunikacji Polskiej jest to adres cert@telekomunikacja.pl bądź formularz na stronie Zgłaszanie incydentu).

Adres IP (Internet Protocol) - to cyfrowy „adres", inny dla każdego komputera w Internecie, pozwalający na jego jednoznaczną identyfikację. Np. adres serwera tp.pl to 217.97.216.10. Adres IP może być stały lub tzw. dynamiczny, inny przy każdym połączeniu z siecią.

Bot (od: robot) - nazwy tej używamy głównie w stosunku do komputerów, zarażonych przez złośliwe oprogramowanie, wykonujących bez wiedzy użytkownika zadania, zlecone przez sieciowych przestępców.

Botnet - wiele komputerów, opanowanych przez boty (tzw. komputerów zombie), połączonych wbrew wiedzy swoich właścicieli w sieć. Siecią zarządzają przestępcy, za pośrednictwem serwera kontrolującego (Command&Control, C&C). Botnety najczęściej wykorzystywane są do przeprowadzania zmasowanych ataków blokowania dostępu do wybranych przez przestępcę stron bądź rozsyłania spamu.

CERT (Computer Emergency Response Team) - zespół szybkiego reagowania na zagrożenia komputerowe. Prawo do używania nazwy CERT mają wyłącznie zespoły spełniające bardzo wysokie wymagania. W Polsce są to: działający w ramach Telekomunikacji Polskiej TP CERT, CERT Polska, CERT.gov.pl oraz Pionier-CERT.

Cracker - osoba, która celowo chce dokonać jak największych zniszczeń poprzez rozsyłanie wirusów, włamywanie się i kasowanie danych. Niekoniecznie musi mieć wąską wiedzę z dziedziny bezpieczeństwa – tzw. script-kiddies korzystają z gotowych zestawów narzędzi służących do przełamywania zabezpieczeń.

Cracking - łamanie zabezpieczeń systemu (np. haseł), przy wykorzystaniu znalezionej luki w zabezpieczeniach, najczęściej przy pomocy specjalnych programów (tzw. exploitów i/lub cracków). Hasła łamie się najczęściej za pomocą ataków słownikowych (program sprawdza hasła z listy najpopularniejszych) oraz brutalnej siły (tzw. brute force, program wprowadza wszystkie możliwe hasła po kolei).

Czarne listy - zbiory danych o adresach IP komputerów, wysyłających spam. Serwery pocztowe po prostu nie wpuszczają e-mail z adresów umieszczonych na czarnej liście. Dla odmiany białe listy zawierają zaufane adresy serwerów.
Firewall (ściana ogniowa/zapora sieciowa) - kontroluje przepływ informacji między Internetem i Twoim komputerem lub siecią lokalną. Zapobiega standardowym atakom, pomaga rozpoznać i powstrzymać próbę włamania oraz blokuje niepożądany ruch. Na domowym komputerze stosuje się w tym celu programy, zaś Twój dostawca Internetu (np. Telekomunikacja Polska) używa w tym celu specjalnych urządzeń.
Haker - osoba z bardzo szeroką wiedzą informatyczną, dla której wyzywaniem jest poszukiwanie nowych możliwości przełamywania zabezpieczeń. Hacker często mylony jest z crackerem, bowiem nie działa ze złej woli, po prostu lubi to, co robi, a po odkryciu luki w zabezpieczeń informuje o niej np. producenta programu czy administratora strony.
Hotspot - dostępny publicznie punkt bezprzewodowego dostępu do internetu (WiFi), dzięki któremu możesz podłączyć się do sieci telefonem czy laptopem. Hotspoty mogą być bezpłatne lub płatne, najczęściej znajdziesz je w takich miejscach, jak centra handlowe, w szkoły i uczelnie, centra miast, hotele czy na lotniska.
Keylogger - rejestruje znaki wpisywane z klawiatury komputera i wysyła je do przestępcy, np. operatora botnetu. W ten sposób przestępca może przechwytywać wpisywane na Twoim komputerze hasła, loginy i inne istotne dane.
Koń trojański, trojan - program, umożliwiający zdalne przejęcie kontroli nad komputerem, może być „zaszyty" w programach z niezaufanych stron internetowych, wygaszaczach ekranu, a nawet specjalnie spreparowanych obrazkach jpg. Przestępca po przejęciu kontroli nad komputerem może wydawać mu polecenia, podsłuchiwać komunikację z innymi komputerami, przechwytywać hasła, przejąć sterowanie podłączonymi do niego urządzeniami czy też rozsyłać spam. Może zostać zainstalowany bez Twojej wiedzy (wykorzystując luki w bezpieczeństwie systemu) lub... przez Ciebie, jeśli przestępca przekona Cię do uruchomienia niewinnie wyglądającego programu.

Kopia bezpieczeństwa, kopia zapasowa - dzięki regularnemu kopiowaniu ważnych dla Ciebie danych z komputera na płyty DVD bądź zewnętrzne dyski, unikniesz utraty dokumentów czy zdjęć w przypadku uszkodzenia dysku bądź komputera. Przy awarii komputera kopia zapasowa może pozwolić na przywrócenie go do stanu sprzed awarii.
Kradzież tożsamości - sytuacja, gdy ktoś uzyskuje dostęp do Twoich danych (np. z widocznego dla wszystkich profilu na Facebooku) po to, by podszyć się pod Ciebie i dokonać oszustwa (np. kupić towary, używając Twojego konta w serwisie aukcyjnym).
Logi - to spis wszystkiego, co działo się w systemie bądź programie, zazwyczaj zapisywany w pliku. Dzięki logom można np. nadzorować wykorzystanie komputera (sprawdzić kto i kiedy oglądał strony www).
Łańcuszki, fałszywe ostrzeżenia - niegroźne, lecz generujące niepotrzebny ruch w sieci i często siejące panikę e-maile. Często są to np. ostrzeżenia przed nowymi, tak naprawdę nieistniejącymi wirusami, czy też informacje o tym, jakie szczęście (lub pech) spotkało osoby, które już przesłały (bądź nie przekazały) maila dalej.
Mailbombing (bomba e-mail) - wysyłanie ogromnej ilości wiadomości e-mail na określony adres pocztowy, czego skutkiem jest całkowite „zapchanie" serwera lub konta użytkownika.
Malware (malicious software, złośliwe oprogramowanie) - tak nazywamy wszystkie programy (wirusy, robaki, trojany, czy spyware), których celem jest przejęcie kontroli nad komputerem, kradzież zawartych na nim danych (w tym haseł) i inne tego typu działania.

Netykieta - zbiór dobrych zwyczajów, dotyczących komunikacji w Internecie, opracowywany przez społeczność internetową. Ma ułatwić korzystanie z sieci oraz pomóc zrozumieć, czym może się skończyć nieodpowiednie zachowanie (np. zablokowaniem dostępu do zasobów lub usług, których dotyczyło nadużycie).

Pharming - użytkownik jest przekierowywany do podstawionej przez oszusta strony internetowej, podczas, gdy w pasku adresu przeglądarki adres jest prawidłowy – cyber-przestępca zaatakował wcześniej serwer, tłumaczący adresy zwykłe na numeryczne (IP), w efekcie czego fałszywą stronę widzimy pod „prawdziwą" nazwą.

Phishing - oszustwo mające na celu kradzież poufnych danych osobistych (np. numerów kart kredytowych, haseł do stron internetowych). Cyber-przestępca namawia użytkownika do samodzielnego wpisania poufnych danych na „podłożonej" stronie, bardzo podobnej do oryginalnej, najczęściej przysyłając mającego wzbudzić zaufanie e-maila. Adres strony przestępcy jest bardzo podobny do prawdziwego, np. zamiast litery l (el) jest duże i, które wygląda tak samo. Jeśli masz wątpliwości, czy strona, na którą chcesz wejść, jest prawdziwa, wpisz jej adres na stronie http://urlvoid.com/

Programy szpiegujące (spyware) - bez zgody i wiedzy użytkownika zbierają informacje o nim i tym, co robi, korzystając z komputera (np. jakie stron odwiedza, jakie e-maile wysyła, jaką konfiguracje ma jego komputer, a nawet jakie wpisuje hasła), przesyłając je potem do cyber-przestępców. Takie programy mogą też zmieniać konfigurację przeglądarki, by wymuszać przeglądanie stron z reklamami, za które przestępca dostaje pieniądze.

Robak internetowy - młodszy i sprawniejszy brat wirusa komputerowego. To program, który rozpowszechnia się przez sieć w jak największej liczbie kopii. Robaki infekują kolejne komputery, wykorzystując błędy w używanych programach albo systemie, a także nieostrożność użytkowników, którzy np. klikają w podejrzane linki.

Robak może niszczyć Twój komputer, ale może też być koniem trojańskim, który bez wiedzy użytkownika otworzy zabezpieczenia systemu i wpuści do niego inne groźne programy.

Rootkit - jego główne zadanie to ukrywanie innych złośliwych programów przed narzędziami zabezpieczającymi system. Rootkit może się dostać do komputera podobnie jak inne złośliwe programy (np. wraz z trojanem).

Spam. Niechciana przez odbiorcę wiadomość e-mail, rozsyłana anonimowo, z wyłudzonych lub przechwyconych adresów, zazwyczaj przy użyciu botnetów. Spam to najczęściej reklamy różnych usług i produktów.

Spoofing - sytuacja, gdy komputer udaje inny komputer, dzięki czemu może włamać się do systemu lub dokonać oszustwa. Spoofować można adresy e-mail (wtedy w informacji „Od" pojawiają się fałszywe dane), adres IP albo stronę WWW (wtedy ruch z naszego komputera „po drodze" trafia do komputera przestępcy)

Wi-Fi - zestaw standardów bezprzewodowego przesyłu danych, realizowanego drogą radiową. A potocznie mówiąc, jest to po prostu sieć bezprzewodowa, dzięki której możemy podłączyć do internetu komputer albo smartfon.

WWW (World Wide Web, ogólnoświatowa pajęczyna) - wyobraźcie sobie wielką mapę świata i strony internetowe, z których wychodzą linki do innych stron, często w zupełnie innej części świata. To właśnie te linki oplatają naszą planetę niczym ogromna, wirtualna pajęczyna.

Słownik powstał przy współpracy z TP CERT, jednostką reagowania na zagrożenia bezpieczeństwa teleinformatycznego Orange Polska (http://cert.orange.pl).

Szkodliwe treści

Surfując po Internecie, możesz natknąć się na materiały, które są szkodliwe. Do nich zaliczają się różnego rodzaju artykuły, fora internetowe, zdjęcia lub filmy mające charakter **przemocowy**, **pornograficzny** oraz **nawołujący do nietolerancji wobec ludzi innej rasy**, **narodowości** lub **wyznania**. Kontakt z takimi treściami ma negatywny wpływ na psychikę, gdyż tego typu informacje budzą nieprzyjemne skojarzenia, powodują napięcie oraz uderzają w wartości i moralność człowieka.

Szkodliwe treści to przede wszystkim informacje:

Ukazujące pornografię.
Namawiające do wyśmiewania innych z powodu rasy, narodowości lub wyznawanej religii.
Namawiające do popełnienia przestępstwa.
Propagujące faszyzm i totalitaryzm.
Prezentujące przemoc.
Zachęcające do podejmowania działań autodestrukcyjnych, czyli takich, które powodują szkody cielesne lub psychiczne np. uzależnienie.
Zawierające wulgaryzmy.
Zawierające elementy psychomanipulacji, czyli takiego sterowania cudzymi uczuciami, którego celem jest wyłudzenie korzyści materialnych lub zmuszenie do niewłaściwych zachowań.
Wprowadzające w błąd, co może mieć wpływ na życie i zdrowie młodego użytkownika.
Zachęcające do prostytucji, używania narkotyków czy hazardu.

Dlaczego te treści są szkodliwe?

*Oglądanie takich materiałów może sprawić, że świat nagle stanie się niezrozumiały, zagrażający i przestaniesz czuć się w nim bezpieczne.
*Możesz dać się namówić do wyrządzenia komuś krzywdy, w tym także do czynów karalnych.
*Kontakt ze szkodliwymi treściami ułatwia osobom obcym, ze złymi intencjami dotrzeć do Ciebie.
*Kontakt z treściami pornograficznymi zaburza Twój rozwój psychoseksualny, czyli możesz nauczyć się nieprawidłowych zachowań/ wzorców seksualnych.
*Czytanie treści zawierających przemoc czy rasizm może skłonić do zachowań agresywnych wobec rówieśników, słabszych czy ludzi innej narodowości, wyznania.

Jak reagować w sytuacji, kiedy trafisz na stronę ze szkodliwymi treściami?

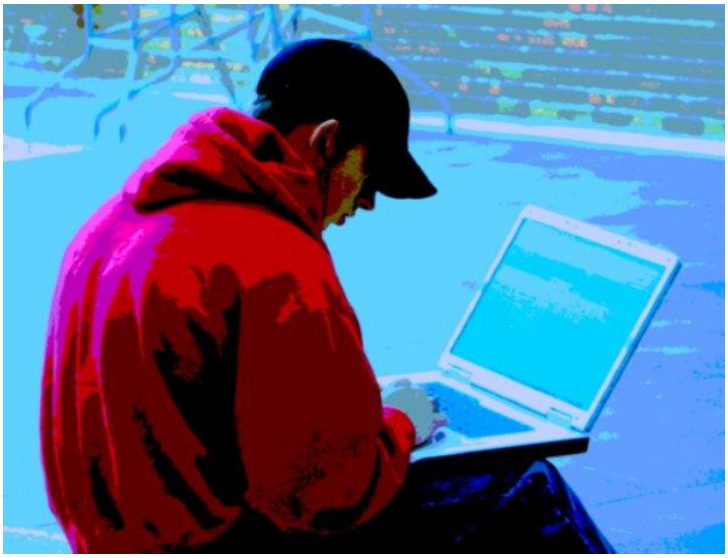
Kontakt ze szkodliwymi treściami może wywołać nieprzyjemne uczucia, to normalne, gdy czujesz zdenerwowanie lub zażenowanie.

Jeśli w czasie surfowania po sieci, natkniesz się na szkodliwe lub niebezpieczne treści , możesz skontaktować się z Helpline.org.pl - telefon 800 100 100 i czat są czynne od poniedziałku do piątku od 11.00 do 17.00
Możesz również napisać na adres hepline@helpline.org.pl lub za pomocą formularza dostępnego na stronie www.helpline.org.pl

Treści nielegalne, które naruszają prawo, czyli:

*opublikowaną w sieci pornografię bez filtra informacyjnego o materiałach tylko dla dorosłych,
*treści rasistowskie,
*treści propagujące totalitaryzm i faszyzm,
możesz zgłosić anonimowo poprzez formularz na stronie www.dyzurnet.pl

Uzależnienie od Internetu, komputera



Czy wiesz, że część użytkowników przebywa online zbyt długo i nie jest w stanie tego kontrolować?
Istnieje wiele wątpliwości co do tego, czy taki stan możemy nazwać uzależnieniem od Internetu, siecioholizmem, patologicznym używaniem czy nadużywaniem tego medium.
Część naukowców uważa, że nie możemy stosować pojęcia "uzależnienie" w odniesieniu do Internetu, gdyż różni się od uzależnienia od narkotyków czy alkoholu. Inni włączają je do grupy tzw. uzależnień behawioralnych, czyli od czynności (np. uzależnienie od hazardu). Jeszcze inni twierdzą, że osoby, które utraciły kontrolę nad korzystaniem z Internetu, używają go w sposób patologiczny bądź po prostu nadużywają.
Bez względu na to, jakie stanowisko przyjmiemy, faktem jest, że problem istnieje. O tym, jak ostatecznie zostanie nazwany zadecydują wyniki badań, które przeprowadzane są aktualnie w Europie i na świecie.
Jak rozpoznać ten problem?

U osób, które nadużywają Internetu/komputera, może pojawić się:

Silna potrzeba lub poczucie przymusu korzystania z Internetu.
Brak kontroli nad długością czasu spędzanego w sieci.
Problem z powstrzymaniem się od korzystania z Internetu.
Występowanie niepokoju, rozdrażnienia czy gorszego samopoczucia przy próbie przerwania lub ograniczenia korzystania z Internetu oraz ustępowanie tych stanów z chwilą powrotu do sieci.
Zaniedbywanie dotychczasowych zainteresowań oraz kontaktów z ludźmi na rzecz Internetu.
Spędzanie coraz większej ilości czasu w Internecie celem uzyskania zadowolenia, dobrego samopoczucia, które poprzednio osiągane było w znacznie krótszym czasie.
Korzystanie z Internetu pomimo szkodliwości poświęcania tak długiego czasu na jedną aktywność.

Pamiętaj!!!

Tylko specjalista może stwierdzić, czy dana osoba jest uzależniona od Internetu.
Jeśli rozpoznajesz podobne objawy u siebie – porozmawiaj z kimś bliskim w domu lub szkole.

Konsekwencje nadużywania Internetu:
Zaniedbywanie nauki oraz codziennych obowiązków.
Zaburzenia w sferze uczuć i emocji np. częste uczucie niepokoju, agresja.
Brak troski o własne zdrowie (brak snu, brak ruchu, nieregularne posiłki) i higienę osobistą.
Wyobcowanie z realnego świata.
Problemy w relacjach z ludźmi, unikanie kontaktu z ludźmi w świecie realnym, konflikty.
Rezygnacja z zainteresowań i przyjemności.
Trudności z koncentracją.
Problemy zdrowotne (pogorszenie wzroku, bóle głowy, niedożywienie, zaburzenia snu, nieprawidłowy oddech, zespół kanału nadgarstka, skrzywienia kręgosłupa).

Zastanów się!

- **Czy czujesz się zaabsorbowany Internetem (myślisz o poprzednich bądź następnych pobytach w sieci)?**
- **Czy czujesz potrzebę używania Internetu przez coraz dłuższe okresy czasu?**
- **Czy wielokrotnie miałeś nieudane próby kontroli, ograniczenia czasu lub zaprzestania korzystania z Internetu?**
- **Czy czułeś się niespokojny, markotny, zirytowany, przygnębiony gdy próbowałeś ograniczać czas w Internecie lub zaprzestać korzystania z niego?**
- **Czy pozostajesz w sieci dłużej niż pierwotnie planowałeś?**
- **Czy ryzykujesz utratę ważnych relacji, prac, możliwości kariery lub nauki z powodu Internetu?**
- **Czy oszukałeś kogoś z rodziny, bliskich lub terapeutów, aby ukryć narastający problem Internetu?**
- **Czy używasz Internetu jako sposobu na ucieczkę od problemów lub sposobu na pogorszony nastrój (uczucia bezradności, winy, lęku, depresji)?**

DZIEŃ BEZPIECZNEGO INTERNETU W NASZEJ SZKOLE

Razem tworzymy lepszy Internet ☺

To hasło towarzyszyło w tym roku ogólnopolskim obchodom Dnia Bezpiecznego Internetu. W naszej szkole trwały one do połowy marca. W tym czasie odbywały się różne działania profilaktyczne.

Uczniowie klas: I TC, I TD, I TE, II TE, II TB wzięli udział w spotkaniu z policjantem Komendy Powiatowej Policji w Gostyniu panem Grzegorzem Błaszczykiem. Było ono poświęcone zjawisku cyberprzemocy i ogólnie pojętemu bezpieczeństwu w sieci.
Prelekcję uzupełniły filmy, które przygotowała pedagog Katarzyna Kozłowska. Obrazowały one omawiane zjawiska. Spotkanie zorganizowali pedagodzy szkolni.

Czy to mamy komputer i Internet, czy też komputer i Internet mają nas?

Uczniowie klas IC, IB, II TE, II D, I TE, II C wzięli udział w spotkaniu z psychologiem Poradni Psychologiczno – Pedagogicznej w Gostyniu panią Agnieszką Woźnicą, która próbowała odpowiedzieć na pytania: czy samotność w sieci jest możliwa i czy to my mamy komputer i Internet czy też komputer i Internet mają nas? Pani psycholog uświadamiała uczniom, że w wirtualnym świecie łatwo zafałszować rzeczywistość albo ulec urokowi pozornie bezproblemowego życia. Zwróciła również uwagę na to, czym różni się normalne korzystanie z komputera i Internetu od tego problematycznego i chorobliwego. Organizatorem spotkania była pani Bogusława Skoracka i pedagodzy szkolni.

Komórka to nie kumpel – przyjaźnij się z ludźmi!

Przy okazji obchodów Dnia Bezpiecznego Internetu w naszej szkole podjęty został również temat bezpiecznego korzystania z telefonów komórkowych.

Bezpieczne korzystanie z telefonów komórkowych, fonoholizm, czyli uzależnienie od telefonu komórkowego, szkodliwość promieniowania elektromagnetycznego to wszystko było tematem spotkania, jakie przeprowadziły: pielęgniarka Agnieszka Włodarczak i pedagog Katarzyna Kozłowska. W prelekcji uczestniczyli uczniowie z dziewięciu klas: I TA, I TC, I TD, ITE, II TA, II TB, II TC, III TA, III TC.

Czy wiesz co to jest Netykieta?

Netykieta to zasady dobrego zachowania w Internecie:
Zwracając się do konkretnego internauty, pamiętaj o używaniu dużej litery w zaimkach: Ty, Tobie, Ci itp.
Staraj się nie nadużywać emotikonek (uśmieszków, buziaczków).
Staraj się nie używać dużych liter, bo oznaczają podniesiony głos lub KRZYK.
Gdy jesteś nowym użytkownikiem na forum, sprawdź, czy na Twoje pytanie nie udzielono już odpowiedzi. Zanim zadasz pytanie, sprawdź, czy nie ma odpowiedzi w FAQ (ang. Frequently Asked Questions – najczęściej zadawane pytania).
Nie zaśmiecaj Internetu niepotrzebnymi informacjami lub takimi, które już tam są.
Nie obrażaj innych użytkowników sieci – staraj się zachowywać w sposób kulturalny.
Szanuj wpisy innych internautów.
Masz prawo do wyrażania swoich poglądów, pamiętaj, że inni też mają takie prawo.
Jeżeli cytujesz wypowiedzi czy korzystasz z czyichś prac – zawsze podawaj źródło.
Nie zakładaj sobie niepotrzebnych kont e-mail.

Nr 81 Schizola przygotowała
Katarzyna Kozłowska pedagog
Skład: Alicja Gorynia
Leszek Niemczyk

Adres do korespondencji:
Zespół Szkół Zawodowych
im. Powstańców Wielkopolskich
SCHIZOL
ul. Tuwima 44
63-800 Gostyń