Informator dla nauczycieli, uczniów, ich rodziców o kształceniu na odległość w szkole, z uwzględnieniem higieny pracy uczniów i nauczycieli oraz zasad bezpieczeństwa w sieci

Kształcenie na odległość w szkole

Kiedy mówi się o kształceniu na odległość, najczęściej można usłyszeć czy przeczytać zdanie, że jest to forma, w której można się uczyć 24 godziny na dobę, 7 dni w tygodniu, bowiem pracując online mamy stały dostęp do materiałów dydaktycznych i w każdej chwili możemy skontaktować się z nauczycielem czy innymi uczestnikami zajęć. Rzeczywiście, ucząc się przez Internet, mamy większą swobodę czasową, ale… trzeba pamiętać o tym, że nauczyciel nie czeka na uczniów całą dobę, a i oni muszą tak zorganizować sobie własny dzień, żeby znaleźć czas na pracę, sprawy rodzinne, hobby i naukę. Zarządzanie czasem przeznaczonym na pracę online jest z pewnością wyzwaniem dla nauczyciela, jak i dla osoby uczącej się online. Każdy bowiem sam decyduje, ile czasu musi spędzić w obszarze kursu online, by wypełnić wszystkie obowiązki. Umiejętność dobrego zarządzania daje możliwość opanowania dwóch niezwykle istotnych czynności. Po pierwsze — umiejętności szybkiego zrealizowania swoich zadań. Po drugie — umiejętności ustalania priorytetów i organizowania swojego dnia tak, żeby wykonywanie codziennych

obowiązków nie kolidowało z kształceniem na odległość. Nowe środowisko nauki, jakim jest kształcenie na odległość, wymaga wyrobienia nowych zachowań — bez względu na to, czy jest się nauczycielem, czy uczniem, trzeba nauczyć się na niej pracować i racjonalnie wykorzystywać swój czas. Zmieniające się w procesie nauki zdalnej zadania nauczyciela powodują, że nie jest on już tak skoncentrowany na przekazywaniu wiedzy (jak ma to miejsce w tradycyjnej edukacji), ale staje się osobą motywującą i angażującą uczniów do pracy online i nauki poza nią. Dlatego istotne jest takie rozplanowanie sobie wszystkich zajęć, by móc sprawdzać, co dzieje się na bieżąco. Najlepiej jest ustalić sobie stały rozkład tygodnia i, biorąc pod uwagę inne swoje zajęcia i obowiązki, przeznaczyć czas na pracę, np. w poniedziałki, środy i soboty, w określonych godzinach. Czas ten powinien wystarczyć na przeczytanie postów na forach, skomentowanie ich i ocenę, sprawdzenie i ocenienie prac domowych, projektów itd. Gdy jednak jest się początkującym e-nauczycielem praca na platformie wymaga większego zaangażowania, choćby dlatego, że trzeba dobrze poznać środowisko nauki i nauczyć się sprawnie komunikować online — czy to poprzez fora dyskusyjne i czaty, czy poprzez e-maile. Trzeba pamiętać, że zastąpienie komunikacji bezpośredniej, odbywającej się twarzą w twarz, tekstem zapisanym wymaga pewnej wprawy i dłuższego czasu na sformułowanie w piśmie swoich myśli, tak, by były jednoznaczne i nie pozostawiały pola do domysłów, czy też różnych interpretacji. Równie ważne, jak w wypadku pracy nauczyciela, jest planowanie sobie czasu przez ucznia. Pozostawianie nauki na ostatnią chwilę prowadzi najczęściej do sytuacji spiętrzenia się zadań i obowiązków, a to prosta droga do kłopotów i niepotrzebnego stresu! Dlatego tak ważne jest, by zaraz po rozpoczęciu nauki online, uczeń zapoznał się z harmonogramem kursu online — jest to kalendarz pracy, który szczegółowo wskazuje daty (a czasami nawet godziny) realizacji poszczególnych etapów kursu i występujących w nim zadań i prac. Każdy uczeń musi samodzielnie przeanalizować swój rozkład dnia i zastanowić się, w jakie dni, w jakich godzinach jest w stanie poświęcić czas na pracę online. I tu warto (jak w przypadku pracy nauczyciela) zarezerwować sobie na te czynności wybrane dni tygodnia i wolne dotąd godziny. Podsumowując podczas zajęć online, trzeba pamiętać, że niezależnie od tego, czy jesteśmy nauczycielem, czy uczniem należy: – Określać swoje priorytety!

Jeśli jesteś nauczycielem, zaplanuj, co zrobisz najpierw — czy w danym dniu będziesz sprawdzać prace domowe, czy może skupisz się na pracy na forum dyskusyjnym? A może poświecisz swój czas na motywowanie i aktywizowanie uczniów? Jeśli uczysz się online, nie możesz traktować nauki jako zajęcia małoistotnego, na które kiedyś „znajdziesz chwilę" — by z sukcesem ukończyć zajęcia musisz mieć czas, a więc zaplanować swoją naukę i wpisać ją w swój tygodniowy plan! – Analizować, ile czasu poświęca się na wykonanie danego zadania! Każda czynność, która wykonywana jest wielokrotnie, zajmuje nam określony czas. Jeśli zaczniesz zwracać uwagę na to, ile minut zwykle poświęcasz na przejrzenie forum i zamieszczenie na nim postu, ile minut zajmuje zrobienie, czy sprawdzenie pracy domowej, pomoże Ci to lepiej zaplanować swój czas w kolejnych tygodniach spędzonych na prace online.

Organizacja nauki

Aktualnie wszystkie szkoły prowadzą nauczanie zdalnie umożliwiając uczniom dostęp do materiałów dydaktycznych za pośrednictwem różnych platform e-learningowych czy poprzez z wykorzystaniem komunikatorów, grup społecznościowych, poczty elektronicznej, W ten sposób uczniowie kontaktują się z nauczycielami. Zgodnie z wytycznymi realizują zadania, przerabiają materiał z listy przedmiotów obowiązkowych, także w zakresie edukacji wczesnoszkolnej. Pomoce dydaktyczne w interaktywnej formie sprawiają, że nauka staje się przyjemna bez względu na wiek ucznia. Wszystko to sprawia, że uczniowie wykazują dużą chęć do nauki.

Gdzie szukać informacji o zdalnej pracy z uczniami?

Minister Edukacji Narodowej zachęcił dyrektorów do skorzystania z dostępnych stron internetowych, rekomendowanych przez MEN, na których znajdują się materiały i wskazówki do pracy zdalnej z uczniami, m.in.: www.epodreczniki.pl, www.cke.gov.pl (i stron Okręgowych Komisji Egzaminacyjnych), www.gov.pl/zdalnelekcje, a także informacji dostępnych na stronie ministerstwa edukacji www.men.gov.pl.

Aby pomóc nauczycielom i dyrektorom szkół w organizacji zajęć edukacyjnych z wykorzystaniem metod i technik kształcenia na odległość w najbliższych dniach przekażemy dyrektorom materiały informacyjne dotyczące zdalnego nauczania.

Warto przypomnieć, że wczoraj opublikowaliśmy kompleksowe zestawienie najważniejszych informacji, a także linków do stron internetowych, które mogą być wykorzystywane przez nauczycieli i dyrektorów szkół do przygotowania materiałów do samodzielnej pracy uczniów w domu. https://www.gov.pl/web/edukacja/lekcje-z-internetu

Wymagania sprzętowe

Nauka wykorzystująca technologie informatyczne w postaci platform e-learningowych nie wymaga na ogół żadnego specjalistycznego sprzętu komputerowego. Lekcje zazwyczaj udzielane są za pośrednictwem łączy internetowych, a minimalne wymagania sprzętowe nie są wygórowane. Nie obejdzie się oczywiście bez kamery internetowej i słuchawek z mikrofonem. Przydatne będą drukarka i skaner.

Kształcenie na odległość a higiena pracy uczniów i nauczycieli

W procesie nauczania –uczenia się, niezwykle ważnym zagadnieniem jest higiena pracyumysłowej ucznia i nauczyciela.Organizacja nauki online to czynniki, które w istotny sposób wpływają na postępy w uczeniu się.Możliwości percepcyjne uczniów najmłodszych różnią się znacznie od możliwości uczniów starszych. Ustalono, że dzieciw wieku 7 –10 lat mogą skupić uwagę na lekcji przez około 20 minut. W wieku 15 lat czas ten przedłuża się do 30 minut. Przemęczenie powstaje po wysiłku długotrwałym, nawet niezbyt intensywnym, ale nieprzerywanym chwilami odpoczynku. Pierwszymi objawamizmęczeniauczniów są: rozproszenie uwagi, nadmierna pobudliwość, drażliwość i żywość, pobudzenie ruchowe,które mogą następnie przejść wobjawy apatii, senności oraz brak zdolności skupiania uwagi. Podobnie nauczyciele odczuwają zmęczenie. Aby zapobiec występowaniu tych objawów należy stosować przerwy w nauce iodpowiednio je wykorzystywać poprzez relaks i wypoczynek, ale również dostęp świeżego powietrza w pomieszczeniu do nauki domowej w odniesieniu do ucznia i nauczyciela. Niezmiernie ważnym

elementem higienicznym jest racjonalny tryb życia ucznia, który regulowany prawidłowym rozkładem organizacyjnym dnia wdraża do systematyczności oraz nawyków higienicznych. W rozkładzie dnia powinno przestrzegać się przede wszystkim prawidłowej proporcji między trzema elementami: snem, zajęciami ruchowymi oraz nauką.Oczywiście rozkład dnia ucznia w dużym stopniu jest wyznaczony przez obowiązki szkolne. Senpowinien odbywać się tylko w nocy od godziny 20 –tej dla dzieci młodszych i od 20.30, 21.00 dla dzieci starszych itrwać:

- 9-11 godzin na dobę-dzieci w wieku szkolnym (6-13 lat)
- 8-10 godzin-nastolatki (14-17 lat) Drzemki kilkudziesięciominutowe po nauce w szkole mogą być higienicznie uzasadnione, jednak sen kilkugodzinny w ciągu dnia jest niewskazany, narusza bowiem rytm biologiczny aktywności dziecka. W obecnej sytuacji epidemiologicznej dzieci, młodzież i nauczyciele powinni skorzystać ze spaceru w odosobnionym od innych ludzi miejscu. Jeśli to zupełnie niemożliwe wówczas należy wyjść na balkon czy taras i pospacerować. Nauka w domupowinna byćracjonalniezorganizowana. Wymagatood ucznia i nauczyciela nie tylko dobrej znajomości zadań, jakie ma do wykonania, ale też orientacji, jaką wybrać taktykę, jak ukierunkować przebieg swojej nauki wdomu.

Wskazane jest następujące rozłożenie odrabiania pracy domowej:

- odrabianie na przemian zadań trudnych i łatwych, co zapobiegnie szybkiemu zmęczeniu,

- przeplatanie zadań pisemnych ustnymi,

- przechodzenie do odrabiania zadań z następnego przedmiotu dopiero po dokładnym opracowaniu materiału z przedmiotu przygotowanego poprzednio.

Regulamin odrabiania pracy domowej:

1. Odrabianie zadanych prac zawsze w tym samym czasie, najlepiej między godziną 16-20.2. Odrabianie lekcji w tym dniu, w którym zostały zadane.

2.Równomiernerozkładanie pracy na poszczególne dni tygodnia.

3. W każdym dniu wykonanie najpierw zadań bieżących, po ich ukończeniu przystępowanie do odrabiania zadań okresowych (powtórki, lektura, referaty, sprawozdania).

4. Przed pracą przewietrzenie pokoju, przygotowanie stołu, przejrzenie rozkładu lekcji, przygotowanie potrzebnych podręczników, zeszytów i przyborów do pisania.

5. Po zapoznaniu się z całością pracy, ułożenie jej planu(ustalenie kolejności wykonania zadań, zaplanowanie krótkich przerw między poszczególnymi zadaniami).

6.Pracowanie równomierne, staranne, bez pośpiechu.

7. Po ukończeniu pracy przygotowanie potrzebnychna następny dzień do lekcji książek, zeszytów i przyborów.Uczeń, który będzie posiadał taki regulamin nauki, przyswoi sobie jego zasady ibędzie stosować się do nich, na pewno straci mniej czasu na czynności przygotowawcze, jego praca będzie bardziej efektywna, a tym samym łatwiej ipewniej osiągnie powodzenie szkolne.

Zasady bezpieczeństwa w sieci

Internet nie jest tylko miejscem rozrywki. Za jego pośrednictwem załatwiamy różne ważne sprawy. Dbajmy wówczas, aby niepowołane osoby nie miały dostępu do istotnych informacji. To niełatwe, ponieważ w takcie podróży po sieci mimowolnie pozostawiamy po sobie ślady.

Informacje o nas mogą zostać przechwycone lub pozyskane przez internetowych przestępców. Częściej jednak sami dajemy innym dostęp do nich. Sieć nie mogłaby przecież istnieć bez nadzorujących ją osób. Dostawcy usług internetowych, administratorzy serwisów i programiści umożliwiają nam korzystanie z internetu. Aby efektywniej wykonywać swoją pracę, gromadzą o nas pewne dane. Np. Google

wykorzystuje zbierane informacje, aby dostosowywać wyniki wyszukiwania do użytkownika. Czyni to, m.in. skanując treść e-maili czy zapisując wyszukiwane przez Ciebie frazy.

Używając darmowych narzędzi internetowych często nieświadomie godzimy się na wykorzystywanie naszych danych w różnych celach. Ich krążenie po internecie umożliwia np. rozsyłanie reklamowego spamu. Dlatego też nieraz informacje o nas stają się towarem — są sprzedawane reklamodawcom.

To ważne, by mieć na uwadze poniższe punkty, gdy czatujecie, używacie komunikatora internetowego, czy też udzielacie się na forach dyskusyjnych:

1. Wirus komputerowy

Znaczenie tego określenia jest bardzo szerokie. Stosujemy je do opisywania klasycznych wirusów, ale również robaków, które potrafią samodzielnie się replikować i rozsyłać poprzez pocztę do naszych kontaktów, a także trojanów, które tworzą w systemie dziury pozwalające przedostać się innym rodzajom zagrożeń. Często o wirusach mówi się w kontekście infekcji poprzez nośniki USB, ale mogą one rozpowszechniać się praktycznie w dowolny sposób - wystarczy plik, do którego mogą się dołączyć, mogą być też częścią większego oprogramowania.

2. Hasło zapamiętane w przeglądarce

Rosnąca liczba serwisów, z których korzystamy, to coraz dłuższa lista haseł i loginów, które musimy zapamiętać. By ułatwić sobie życie, pozwalamy zapamiętywać je przeglądarkom internetowym i korzystamy z funkcji autologowania. Z pozoru praktyczne działanie może poskutkować otwarciem przysłowiowej puszki Pandory, gdy nasz komputer lub smartfon wpadnie w niepowołane ręce.

3. Naruszenie prywatności, stalking

Słowo prywatność nabrało w ostatnich latach znacznie większego znaczenia niż kiedyś. I tak jak silnie walczymy o jej nienaruszanie, tak samo często wystawiamy ją

bez obaw na forum publiczne. Chwalimy się szczegółami dotyczącymi naszego życia. Takie informacje mogą wykorzystać cyberprzestępcy czy stalkerzy podszywając się pod znajomych i zachęcając nas do wylewności. Również nasze zdjęcia mogą być wykorzystane przez innych użytkowników sieci, by zaszkodzić na przykład naszemu wizerunkowi.

4. Hakerzy

To grupa ludzi o dużej wiedzy na temat komputerów i technik przedostawania się do różnych systemów komputerowych w czasie rzeczywistym. Ich działania manifestują się jako ataki na nasz komputer i wszelkie inne urządzenia, które mają dostęp do sieci (w tym dyski sieciowe, urządzenia mobilne, multimedialne), oraz próby przejęcia nad nimi kontroli.

5. Spam

Teoretycznie niechciana poczta, bo tym jest spam (określany także jako wiadomości śmieci), powinna być jedynie czynnikiem irytującym. Jednak często w tych pozornie nieszkodliwych treściach kryją się niebezpieczne szkodniki. Cyberwłamywacze liczą, że przez pomyłkę lub z ciekawości otworzymy zainfekowany załącznik, co niestety dość często ma miejsce.

6. Nieodpowiednie treści dla dzieci

Internet pełen jest treści, które nie powinny dotrzeć do maluchów, a zarazem nie są odpowiednio oznaczone. Z kolei ochrona w postaci etykiety "tylko dla dorosłych" czy wymuszenia potwierdzenia wieku jedynie zaciekawi dziecko i wywoła odwrotny do zamierzonego efekt.

7. Pedofilia

Zaburzenie seksualne, które dzięki powszechności internetu stało się wielokrotnie silniejszym zagrożeniem niż przed epoką internetu. Pedofile podejmują działania nawet na powszechnie cenionych stronach i forach. Dzięki anonimowości, jaką daje

internet oraz łatwości stworzenia wirtualnej tożsamości, podszywają się oni pod rówieśników lub osoby dla będące dla młodych użytkowników autorytetami.

8. Bezpieczeństwo danych w sieci

Słowo chmura robi zawrotną karierę, a my coraz chętniej korzystamy z zalet przechowywania w sieci różnorakich danych. Nie tylko zdjęć i filmów, ale również innych tworzonych przez nas treści, niejednokrotnie będących przedmiotem naszej pracy. Korzystanie z usług chmurowych, mimo iż z roku na rok coraz bardziej niezawodne, obarczone jest pewnym ryzykiem, że przechowywane w sieci dane zostaną utracone (na przykład w wyniku awarii pamięci serwera) lub przejęte przez inne osoby.

9. Botnety

To szczególnie nieprzyjemna forma zagrożenia. Dla użytkownika komputera niezauważalna, gdyż oprogramowanie botnetu nie wykonuje działań dla niego szkodliwych (poza ewentualnym wykorzystaniem mocy obliczeniowej i obciążeniem łącza). Grupy zainfekowanych komputerów (zwanych czasem zombie), które tworzą taki botnet, mogą jednak posłużyć do przestępczej działalności. Obecnie botnety, które były niegdyś dużymi strukturami, stają się coraz mniejsze, a przez to coraz trudniejsze do wykrycia i zablokowania.

10. Fałszywe lajki i ciasteczka

W sieciach społecznościowych często podążamy za nawykami znajomych. To znakomita pożywka dla hakerów, którzy umieszczają na stronach kody wymuszające ich polubienie. My widząc na tablicy, że ktoś znajomy polubił interesujący nas temat, klikamy na link i kłopot gotowy.

Z kolei w przypadku powiadomień o ciasteczkach (cookies) czujemy się zobligowani kliknąć i nawet nie sprawdzamy, czy faktycznie zatwierdzamy politykę ciasteczkową, czy coś całkowicie innego. A może się zdarzyć, że klikając na niewinnie wyglądające powiadomienie, zaakceptujemy niekorzystny dla nas regulamin jakiejś usługi.

11. Fałszywe oprogramowanie ochronne

"Twój komputer jest zainfekowany, skorzystaj z naszego oprogramowania" to jedno z haseł kluczy, które w przypadku naiwnych internautów otwiera drogę cyberprzestępcom do komputerów ofiar. Jednakże i ostrożna osoba może stać się ofiarą, gdy zdecyduje się pobrać z internetu jedną z aplikacji antywirusowych, która jest chwalona przez innych internautów. W rzeczywistości taki fałszywy antywirus jedynie udaje działanie prawdziwego programu. Wyświetla nawet udawane komunikaty o wykryciu i usunięciu wirusów, w tle jednak działając na naszą szkodę.

12. Fałszywe witryny i wyłudzanie danych

W tym przypadku najczęściej stosowane jest określenie pharming, czyli podszywanie się pod wrażliwą z perspektywy bezpieczeństwa witrynę, na przykład stronę banku, lub phishing czyli wyłudzanie danych, na przykład poprzez podszywanie się pod znaną osobę lub bazując na ludzkiej empatii. Pharming wykorzystuje techniki oszukiwania systemów DNS, tak, by ruch kierowany był na fałszywe witryny, które choć mają inny adres IP to w przeglądarce identyfikują się takim samym lub bardzo podobnym adresem WWW. Ukrycie fałszerstwa ułatwia podmiana jedynie fragmentu strony, co utrudnia wykrycie adresu złośliwej witryny. Phishing z kolei pozwala osiągnąć podobny efekt, ale w tym przypadku wykorzystywana jest naiwność internauty, od którego bank rzekomo potrzebuje potwierdzenia numeru konta czy danych logowania.

13. Szyfrowanie danych bez naszej wiedzy

Nie chodzi tu o nieumiejętne zablokowanie dostępu do danych na naszym dysku, ale celowe iobliczone na zysk działanie szkodników określanych mianem Cryptolocker. Gdy trafią na komputer, szyfrują przechowywane na nim dane, od właściciela żądając jednocześnie okupu. Po jego wpłaceniu, najczęściej w bitcoinach, które zapewniają anonimowość odbiorcy wpłaty, jest szansa na otrzymanie klucza deszyfrującego. Jednak tylko szansa, gdyż wpłata, dokonana nawet przed upływem wyznaczonego okresu, nie gwarantuje odblokowania danych.

14. Wykradanie danych osobowych

Informacje o nazwie użytkownika, haśle dostępowym do serwisu sieciowego, a także powiązanych z tymi danymi, numerem konta czy adresem zamieszkania, od strony dostawcy usług przechowywane są teoretycznie w maksymalnie zabezpieczonej formie. Jednakże coraz częściej dochodzi do przejęcia takich baz danych przez cyberprzestępców.

15. Skrócone adresy

Kolejna forma ułatwienia życia w bogatym w treści Internecie, którą chętnie wykorzystują przestępcy. Adresy stanowiące skróconą alternatywę dla długich oryginalnych adresów, są łatwiejsze do zapamiętania, zajmują mniej miejsca w korespondencji. Zarazem jednak nie wskazują jednoznacznie, dokąd prowadzą, a często kierują do szkodliwej witryny.

16. Literówki w adresach WWW

Wpisując szybko adres strony na klawiaturze nietrudno o pomyłkę, przestawienie liter lub zapomnienie o wpisaniu danego znaku. I choć szanujący się operatorzy witryn sieciowych dbają o rejestrację podobnie brzmiących adresów, nie jest to regułą. Zresztą liczba alternatyw jest tak duża, że trudno przewidzieć jak pomyli się internauta. Otworzenie witryny o podobnie brzmiącej nazwie czasem prowadzi do nic nieznaczącej strony z reklamami, ale czasem może kompletnie zablokować komputer.

17. Otwarte sieci Wi-Fi

Niebezpieczne są na dwa sposoby. W pierwszym przypadku dotyczy to konfigurowanych przez nas domowych sieci, które nie są w żaden sposób zabezpieczone i dają dostęp niepowołanym osobom nie tylko do internetu, ale także do naszych danych. Drugi scenariusz to korzystanie przez nas z otwartych sieci Wi-Fi, o których kompletnie nic nie wiemy. Choć tworzenie takich sieci ma służyć ułatwieniu dostępu do internetu, często taka droga na skróty może byĆ opłakana w skutkach,

gdyż kompletnie nie wiemy, kto kontroluje przepływ danych przez taki punkt dostępowy.

18. Ataki ukierunkowane

Jest to ogólne określenie ataku, który wykorzystuje ludzkie przyzwyczajenia i podatność na błędy w pozornie trywialnych sytuacjach. Cybeprzestępcy mogą tak spreparować szkodniki komputerowe, by zmaksymalizować szanse ich uruchomienia. Istotna w tym przypadku jest bardziej znajomość atakowanego i socjotechnika niż wyrafinowanie zastosowanego oprogramowania.

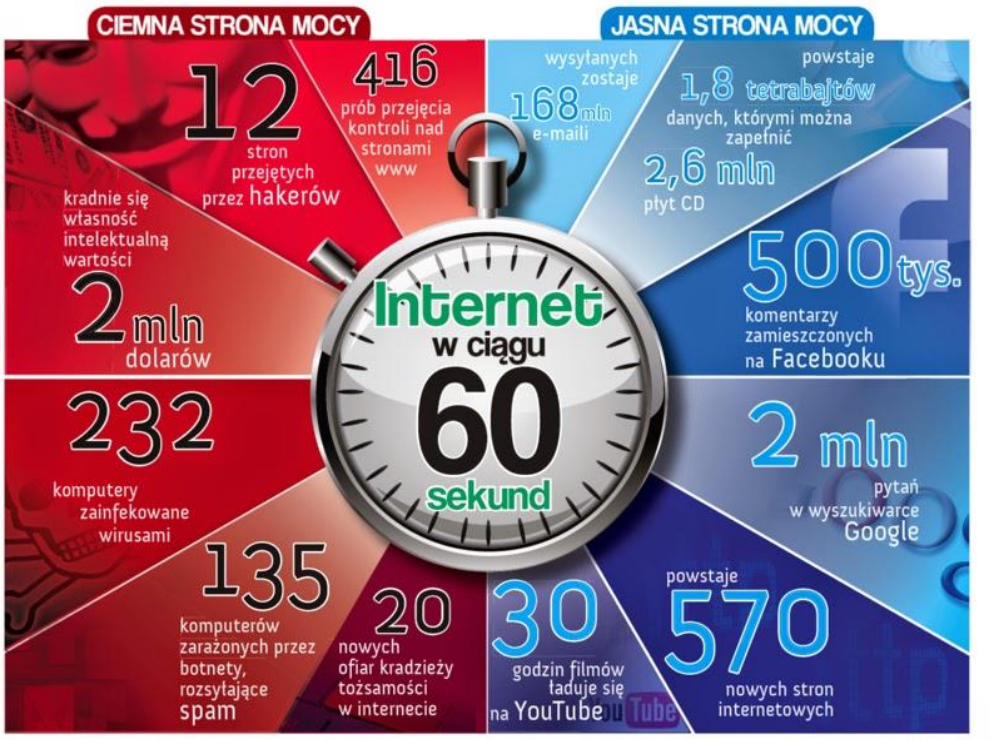
19. Niezaktualizowane oprogramowanie

Wysoki stopień skomplikowania oprogramowania instalowanego na komputerach i innych urządzeniach sprawia, że łatwiej o zaistnienie słabych punktów, czyli dziur. Jeśli nie zostaną one usunięte, na przykład poprzez aktualizację lub nową wersję programu, mogą być wykorzystane przez cyberprzestępców. Dotyczy to nie tylko systemu operacyjnego, ale również wszelkich aplikacji użytkowych, a przede wszystkim pakietów zabezpieczających.

20. Nadmierna wiara w odporność na zagrożenia

Ostatnie z niebezpieczeństw, jakie na nas czyhają, ma swoje źródło w tkwiącej w niejednym internaucie arogancji. Przekonaniu, że doskonale potrafi on sobie poradzić z każdym zagrożeniem. W praktyce często taki człowiek nie zdaje sobie sprawy z różnorodności technik cyberprzestępczych. Jego wiara we własne umiejętności sprawia, że ignoruje rzeczywiste sygnały o zagrożeniu, przedkładając znaczenie innych mało istotnych.

I pamiętajcie, że wszystko zależy od was. Sami decydujecie, w jakie działalności się zaangażować i jakie informacje udostępnić.



Wciąż nie znamy podstawowych reguł bezpiecznego korzystania z sieci. Niestety, nawet najbardziej zaawansowane technologie wykorzystywane przez portale, e-sklepy, poczty e-mail czy banki, nie zabezpieczają nas całkowicie przed zagrożeniami, jakie niesie internet.

Dlatego jednym z najlepszych narzędzi zabezpieczających nasze urządzenia, dane oraz prywatność jest zdrowy rozsądek. Jeśli nie będziemy uważać w jakie linki klikamy, jakie otwieramy załączniki, to na własne życzenie możemy napytać sobie biedy. Oczywiście zainstalowanie pakietu ochronnego (listę najpopularniejszych znajdziecie poniżej) jest bardzo dobrym pomysłem, ale jego używanie nie zwalnia nas z ostrożności.