BEZPIECZEŃSTWO W INTERNECIE

Źródło: https://epodreczniki.pl/

CYBERPRZEMOC

- Cyberprzemoc to rodzaj przemocy przez Internet. Prześladowca straszy, poniża, obraża ofiarę poprzez komentarze w mediach społecznościowych, czy robienie jej zdjęć lub kręcenie filmów bez jej zgody. Następnie materiały umieszcza na ogólnodostępnych witrynach odwiedzanych przez wiele osób. Napastnicy często prześladują i utrudniają życie swoim ofiarom również wysyłając im obraźliwe SMS-y lub e-maile.
- Podobnie jak przemoc fizyczna, cyberprzemoc ma wzbudzić poczucie zagrożenia i zazwyczaj mówimy o dwóch jej rodzajach. Pierwsza dotyczy nieznajomych sobie ludzi. Jej ofiarami padają najczęściej przypadkowe osoby surfujące po sieci internetowej, które trafiają na obraźliwe treści lub czytają przesycone jadem komentarzami pod swoimi wypowiedziami. Atak wymierzony jest najczęściej w członków określonej narodowości, grupy wyznaniowej i zwolenników partii politycznej. Drugą formą przemocy w Internecie jest mobbing elektroniczny, w którym sprawca i ofiara są najczęściej członkami tej samej grupy - coraz częściej
- Doświadczanie jakiegokolwiek ataku, czy to fizycznego czy też psychicznego boli. Cyberprzemoc boli tym bardziej, że jest długofalowa i nieprzerwana. Materiały wykorzystywane podczas ataku są dostępne w krótkim czasie dla wielu osób i jako kopie pozostają w sieci na zawsze, nawet po ustaleniu i ukaraniu sprawcy.
- Źródło: https://bitdefender.pl/

CYBERPRZEMOC - ZAPOBIEGANIE

- 1. Trzeba być ostrożnym w sieci.
- 2. Nie przesyłać zdjęć nieznajomym.
- 3. Nie podawać adresu zamieszkania.
- 4. Nie podawać numeru telefonu.
- 5. Nie umawiać się z nieznajomą osobą na żywo.
- 6. Należy wprowadzić profilaktyczne lekcje w szkole, które uświadomią całej społeczności szkolnej .
- 7. Reagować w gdy zauważy sie na zjawisko cyberprzemocy.
- 8. Podejmować interwencję w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy
- 9. Nie ufaj ludziom obcym z sieci.
- 10. Nie podawaj e – mailu, swojego imienia i nazwiska itp.

- Jeżeli nie wiemy co zrobić z taką sytuacją należy opowiedzieć o tym osobie dorosłej np. rodzicom, nauczycielowi itp.

UZALEŻNIENIE

- Uzależnienie od internetu to zespół zależności mających swoje źródła w nadużywaniu dostępu do internetu, które skutkują negatywnym wpływem na funkcjonowanie jednostki w sferze:
- psychicznej,
- społecznej,
- rodzinnej,
- relacji międzyludzkich,
- ekonomicznej.
- Wielogodzinne, niekontrolowane korzystanie z internetu wywołuje u pacjenta dystres, a więc szereg nieprzyjemnych uczuć:
- ból,
- lęk,
- cierpienie,
- które mogą z kolei prowadzić do znacznego pogorszenia jakości życia. Szkody, które powoduje uzależnienie często dotyczą przy tym nie tylko osoby uzależnionej, ale też jego bliskich i otoczenia.
- Zjawisko jest relatywnie nowe, a jego precyzyjne zdefiniowanie przysparzało naukowcom trudności od samego początku. Świadomość istnienia problemu uzależnienia od internetu upowszechniła się w opinii publicznej i w literaturze fachowej, wciąż jednak brakuje znormalizowanego, ogólnie przyjętego opisu naukowego.

- Źródło: https://www.medicover.pl/

UZALEŻNIENIE - ZAPOBIEGANIE

- Uzależnienie często wynika z poczucia braku. Dla przykładu: młodzież w wieku adolescencyjnym często kontestuje zastaną rzeczywistość, a więc czuje się opuszczona, kiedy musi zweryfikować swoje poglądy. Jeśli rodzice nie rozmawiają z młodym człowiekiem o tym, co czuje, bardzo szybko poszuka on sobie innych znajomych, w Internecie. Warto w takim razie wspierać te zainteresowania, które są możliwie jak najbardziej rozbieżne z koniecznością podłączenia do sieci. Może to być narciarstwo, kajakarstwo czy kolarstwo. Bardzo dobry jest również basen, bowiem nikt nie przyjdzie tam ze smartfonem... chyba, że chce go stracić. Robótki ręczne również są ciekawym sposobem na zabicie czasu i uspokojenie nerwów.
- Warto podkreślać zarówno wady, jak i zalety Internetu. Nadmierne demonizowanie sieci może przynieść skutek odwrotny do zamierzonego, ale merytoryczne wypunktowywanie zagrożeń (np. możliwości dezinformacji) jest już bardzo skutecznym środkiem. Z młodszym dzieckiem należy spędzać jak najwięcej czasu, także wtedy, gdy siedzi ono przy komputerze. Monitorowanie tego, co przegląda i co sprawia mu radość może być kluczem do odkrycia jego zainteresowań. Niewskazane jest natomiast zapisywanie go na ogromną ilość zajęć pozalekcyjnych, byleby tylko nie siedziało przy komputerze. Dzieci mają i tak dużo zadań domowych, toteż obciążanie ich dodatkowym stresem sprawi, że popadną w eskapizm.

Źródło: https://zdrowie-zycie.pl/

NIEBEZPIECZNE TREŚCI

- Do niebezpiecznych treści zaliczamy filmy, zdjęcia, informacje zawierające elementy szkodliwe dla rozwoju psychicznego i emocjonalnego młodego człowieka. Są to materiały pornograficzne, obrazy i filmy prezentujące przemoc i okrucieństwo, treści ksenofobiczne i rasistowskie, treści promujące zachowania autodestrukcyjne, takie jak: anoreksja, samookaleczenia. To co dla nas jawi się jako jedynie coś niewłaściwego, może mieć silny wpływ na zainteresowania i postawę młodego człowieka, szukającego określenia własnej tożsamości i miejsca w otaczającym go świecie.

Źródło: https://www.gov.pl/

ŁAMANIE PRAWA (HAZARD)

- Gry hazardowe
- Grami hazardowymi są gry losowe, zakłady wzajemne oraz gry na automatach. Gry te uregulowane są w ustawie o grach hazardowych.
- Gra losowa charakteryzuje się tym, że wygranymi są pieniądze lub rzeczy, wynik w szczególności zależy od przypadku, a jej warunki określa regulamin. Hasłem kluczem jest tutaj przypadek. W takiej grze nie Wasze umiejętności, ale łut szczęścia decyduje o tym kto wygra, a więc jest to całkowicie niezależne od Was (pomijając trzymanie kciuków czy inne tego typu sprawy). Jedną z najbardziej znanych gier losowych jest loteria promocyjna. Jeżeli kupujecie napój, a pod nakrętką znajdujecie informację o wygranym tablecie - bierzecie udział właśnie w takiej loterii.
- Stawką w zakładzie wzajemnym również są wygrane pieniężne lub rzeczowe, ale tutaj zadaniem osoby biorącej udział w zakładzie jest właściwe odgadywanie. Przykładem zakładu wzajemnego jest zakład bukmacherski, w którym np. typujesz wyniki Ligi Mistrzów.

Źródło: https://antyweb.pl/

ŁAMANIE PRAWA (HAZARD)

- Zasady i wyjątki
- Zakazane jest reklamowanie oraz promocja m.in. gier cylindrycznych (w tym ruletki), gier w karty (m.in. pokera), gier w kości, zakładów wzajemnych oraz gier na automatach.
- Z powyższego zakazu wyłączone zostały wszelkie loterie.
- Tym samym co do zasady reklama zakładów bukmacherskich na stronie internetowej będzie nielegalna, ale już reklama loterii promocyjnej, w której za zakup czekolady weźmiesz udział w losowaniu nagród będzie zgodna z przepisami.
- Jak to często z prawem bywa są wyjątki i jednym z nich jest dopuszczenie podania informacji o sponsorowaniu przez podmiot prowadzący zakład wzajemny. Jednak informacja ta musi się ograniczyć do nazwy sponsora lub innego oznaczenia, które go indywidualizuje (np. logotyp). Może to mieć miejsce np. w sytuacji gdy sponsorem drużyny piłkarskiej jest bukmacher, wówczas na stronie internetowej tej drużyny w miejscu poświęconemu sponsorom może być umieszczone logo takiej firmy.
- Powyższe zakazy dotyczą szerokiego kręgu osób, zarówno reklamujących, jak i osób czerpiących z tego korzyści, zwykłych osób fizycznych oraz przedsiębiorców.

Źródło: https://antyweb.pl

KRADZIEŻ DANYCH OSOBOWYCH

- Dane osobowe są obecnie cennym towarem rynkowym, poszukiwanym m.in. przez ludzi, którzy chcą je wykorzystać w przestępczych celach. Co więcej, bywają pozyskiwane wieloma różnymi metodami - od bardzo prostych, jak np. wyłudzenie ich od osób, których one dotyczą, po wyszukane, wykorzystujące skomplikowane techniki informatyczne czy środki socjotechniczne. Przepisy karne w tym zakresie nie są natomiast doskonałe i w zbyt małym stopniu chronią osobę, której dane osobowe wykorzystano bez jej wiedzy i zgody, wyrządzając jej szkodę. Takie podstawowe wnioski płyną z konferencji naukowej „Kradzież tożsamości w Internecie", zorganizowanej 22 listopada 2016 r. w Warszawie przez Ministerstwo Spraw Wewnętrznych i Administracji, Generalnego Inspektora Ochrony Danych Osobowych oraz Wydział Administracji i Nauk Społecznych Politechniki Warszawskiej.

Źródło: https://archiwum.giodo.gov.pl/

KRADZIEŻ DANYCH OSOBOWYCH

- O tym, że ktoś przyjął naszą tożsamość, często dowiadujemy się, gdy przychodzi do regulacji powstałych zadłużeń - zgłasza się do nas bank lub komornik.

- By tak się nie stało, możemy podjąć odpowiednie kroki, zastrzegające i zabezpieczające nasze dane. Należy sprawdzać wszelkie portale, na których podajemy informacje z dowodu czy karty. Nie powinniśmy otwierać nieznanych załączników, odpisywać na podejrzane wiadomości SMS, dokonywać płatności, jeśli nie jesteśmy w stanie zweryfikować zakupu.

- Zwróćmy też uwagę, w jakich sytuacjach może dojść do przejęcia danych. Wysyłamy je np. gdy pracujemy zdalnie, na umowę o dzieło lub zlecenie, a informacje (imię, nazwisko, PESEL itd.) przekazujemy pocztą elektroniczną. Wiadomość można zaszyfrować na różne sposoby - chociażby sam plik Word czy Excel zabezpieczyć hasłem.

- Kradzież tożsamości w sieci to również przejmowanie przez przestępców naszych kont na portalach społecznościowych. Pamiętajmy, żeby nie przekazywać przez nie istotnych danych i korzystać np. z dwustopniowej weryfikacji (hasło i kod SMS). Zaznaczmy także opcję weryfikacji urządzeń, na których dochodzi do logowania.

Źródło: https://www.praca.pl/

WŁAMANIE KOMPUTEROWE

- Zacznijmy od krótkiego wyjaśnienia kim jest haker oraz jakie grupy hakerów możemy wyróżnić. Przede wszystkim haker jest osobą o wysokich kompetencjach informatycznych. W środowisku programistycznym przyjął się podział dzielący hakerów na:

- białe kapelusze (osoby często pracujące jako audytorzy bezpieczeństwa - zajmują się testowaniem zabezpieczeń informatycznych),
- szare kapelusze (osoby testujące zabezpieczenia nielegalnie, jednak niedomagające się wynagrodzenia w zamian za pozyskane dane),
- czarne kapelusze (przestępcy komputerowi, zajmujący się wykradaniem danych).

- W tym artykule skoncentrujemy się na hakerach działających niezgodnie z prawem, czyli przestępcach komputerowych.

- Ochrona komputerów firmowych przed atakami hakerskimi zabezpiecza nie tylko wrażliwe dane Twojej firmy, ale i prywatne dane pracowników oraz klientów. Statystycznie ponad 60% ataków komputerowych ma związek z błędami użytkowników, którzy nieodpowiednio zabezpieczają swoje sprzęty lub korzystają z rozwiązań, które otwierają drogę dostępu hakerom. Korzystanie z dostępnych rozwiązań prewencyjnych i umiejętność wczesnego rozpoznania „objawów" ataku hakerskiego mogą ochronić Twoją firmę przed problemami. Po czym poznać włamanie na komputer i co zrobić w takiej sytuacji?

Źródło: https://securitypartners.pl/

WŁAMANIE KOMPUTEROWE - ZAPOBIEGANIE

- Jedna z najważniejszych zasad ochrony danych firmowych to regularne wykonywanie kopii zapasowych. Nie ma nic gorszego, niż utrata danych w wyniku ataku hakerskiego i przekonanie się, że pomimo usilnych prób najlepszych informatyków dane są już nie do odzyskania. Kopie zapasowe to podstawa działania komputerów firmowych i prywatnych. Jak mawiają specjaliści IT, użytkownicy komputerów dzielą się na dwie grupy: tych, którzy robią kopie zapasowe i tych, którzy zaczną gdy raz stracą wszystkie ważne pliki.

- Kopia zapasowa to także najlepsze narzędzie do przywrócenia danych po ataku hakerskim. Wielokrotnie okazuje się, że po infekcji komputera konieczne jest usunięcie wszystkich danych i plików oraz całkowite przeinstalowanie systemu operacyjnego, najlepiej na wszystkich komputerach firmowych.

- Przed włamaniami na komputer chronią też oczywiście dedykowane programy antywirusowe i wdrożone rozwiązania ochronne, w tym te monitorujące każdą odwiedzaną stronę internetową i ściąganą, zainstalowaną aplikację. Wyczul swoich pracowników na to, by przed pobraniem czegokolwiek upewnili się o wiarygodnym pochodzeniu aplikacji czy pliku - wiele ataków hakerskich dociera do komputerów przez zawirusowane pliki z fakturami, które z pozoru przypominają te od operatorów sieci komórkowej czy internetowej.

Źródło: https://securitypartners.pl/

ZAGROŻENIA TECHNICZNE (WIRUSY)

- Wirus komputerowy - program komputerowy posiadający zdolność powielania się, tak jak prawdziwy wirus, stąd jego nazwa. Wirus do swojego działania potrzebuje i wykorzystuje system operacyjny, aplikacje oraz tożsamość użytkownika komputera. Wirusa komputerowego zalicza się do szkodliwego oprogramowania (malware).

Źródło: https://pl.wikipedia.org/

ZAGROŻENIA TECHNICZNE (WIRUSY) - ZAPOBIEGANIE

- Korzystaj z aplikacji chroniącej przed złośliwym oprogramowaniem – zainstalowanie i regularne aktualizowanie aplikacji zabezpieczającej ułatwia ochronę komputera przed wirusami i innymi rodzajami złośliwego oprogramowania. Aplikacje chroniące przed złośliwym kodem skanują komputer w poszukiwaniu wirusów, programów szpiegujących i innego złośliwego oprogramowania próbującego zainfekować pocztę e-mail, system operacyjny lub pliki. Nowe zagrożenia mogą pojawiać się codziennie, więc należy regularnie sprawdzać w witrynie internetowej producenta oprogramowania chroniącego przed złośliwym kodem, czy są dostępne aktualizacje.
  Nie otwieraj wiadomości e-mail od nieznanych nadawców ani załączników wiadomości e-mail, których nie rozpoznajesz – wiele wirusów jest dołączonych do wiadomości e-mail i będzie się rozprzestrzeniać zaraz po otwarciu załącznika. Najlepiej nie otwierać żadnego załącznika, o ile nie jest on oczekiwany.

- Korzystaj z funkcji blokowania wyskakujących okienek za pomocą przeglądarki internetowej – wyskakujące okienka to małe okna przeglądarki wyświetlane na tle przeglądanej witryny internetowej. Chociaż większość z nich jest tworzona do celów reklamowych, to mogą także zawierać złośliwy lub niebezpieczny kod. Blokowanie wyskakujących okienek może uniemożliwić wyświetlanie niektórych lub wszystkich takich okienek.

- Pamiętaj o aktualizacji systemu Windows – firma Microsoft okresowo wydaje specjalne aktualizacje zabezpieczeń, które pomagają chronić komputer. Te aktualizacje mogą pomóc w zapobieganiu atakom wirusów i innego złośliwego oprogramowania, niwelując ewentualne luki w zabezpieczeniach.

  Możesz włączyć usługę Windows Update, aby mieć pewność, że system Windows będzie automatycznie otrzymywał te aktualizacje.

- Korzystaj z zapory – zapora systemu Windows lub dowolna inna aplikacja zapory może powiadamiać o podejrzanych działaniach, gdy wirus lub robak próbuje połączyć się z komputerem. Może to także blokować wirusy, robaki i intruzów wysyłających potencjalnie szkodliwe aplikacje na Twój komputer.

- Korzystaj z ustawień prywatności przeglądarki internetowej – w przypadku niektórych witryn internetowych Twoje informacje osobiste mogą być używane do ukierunkowanej reklamy, oszustw i kradzieży tożsamości.

- Upewnij się, że funkcja Kontrola konta użytkownika (UAC) jest włączona – jeśli na komputerze mają zostać wprowadzone zmiany, które wymagają uprawnień na poziomie administratora, Kontrola konta użytkownika informuje o tym i umożliwia zatwierdzenie tej zmiany. Kontrola konta użytkownika może zapobiegać wprowadzaniu niepożądanych zmian przez wirusy. Aby otworzyć funkcję Kontrola konta użytkownika, szybko przesuń od prawej krawędzi ekranu do środka, a następnie naciśnij pozycję Wyszukiwanie. (Jeśli używasz myszy, wskaż prawy górny róg ekranu, przesuń wskaźnik myszy w dół, a następnie kliknij panel Wyszukiwanie). W polu wyszukiwania wpisz wyrażenie kontrola konta użytkownika, a następnie naciśnij lub kliknij pozycję Zmień ustawienia kontroli konta użytkownika.

- Wyczyść internetową pamięć podręczną i historię przeglądania – większość przeglądarek przechowuje informacje o odwiedzonych witrynach internetowych i podane przez Ciebie informacje, takie jak Twoje imię i nazwisko oraz adres. Przechowywanie tych informacji na własnym komputerze może być pomocne, jednak istnieją sytuacje, w których może być potrzebne całkowite lub częściowe usunięcie tych danych (na przykład w sytuacji, gdy korzystasz z komputera publicznego i nie chcesz pozostawiać na nim informacji osobistych).

Źródło: https://support.microsoft.com/

WYŁUCZANIE POUFNYCH INFORMACJI

- Wyłudzanie danych jest przestępstwem polegającym na oszukiwaniu ludzi w celu uzyskania od nich poufnych informacji, takich jak hasła i numery kart kredytowych. Podobnie jak w przypadku łowienia ryb istnieje więcej niż jeden sposób na zanęcenie ofiary, ale jedna taktyka phishingu jest najbardziej powszechna. Ofiary otrzymują wiadomość e-mail lub tekstową imitującą lub podszywajacą się po osobę lub organizację, której ufają, np. współpracownika, bank lub urząd. Gdy ofiara otwiera taką wiadomość, znajduje wiadomość, która ma na celu przestraszyć ją i spowodować, że przestanie racjonalnie myśleć. W wiadomości jest zawarte polecenie, aby ofiara udała się na stronę internetową i podjęła natychmiastowe działanie, gdyż inaczej nastąpią jakieś ryzykowne konsekwencje.

Źródło: https://pl.malwarebytes.com/

WYŁUDZANIE POUFNYCH INFORMACJI

- Podstawową kwestią jeśli chodzi o ochronę przed phishingiem jest zachowanie ostrożności przez użytkowników. Jeśli zatrudniasz pracowników, to powinieneś zadbać o to, aby byli oni świadomi zagrożenia związanego z nieprzemyślanym:

- otwieraniem linków znajdujących się w mailach,
- otwieraniem załączników w mailach,
- wchodzeniem na podejrzane strony internetowe.

- W tym celu warto zorganizować w firmie szkolenie na temat phishingu. Tak, aby pracownicy wiedzieli, co robić, kiedy dostaną podejrzaną wiadomość. Żeby nie klikali bez namysłu w linki, które dostają w mailach. Pracownicy powinni mieć zakodowane w swoich głowach, że zanim w cokolwiek klikną, warto się najpierw dwa razy zastanowić, czy nie jest to czasami jakaś "pułapka". Dobre nawyki pracowników z całą pewnością pozwolą zabezpieczyć Twoją firmę przed utratą ważnych informacji.

Źródło: https://www.ekransystem.com/

KONIEC