Zagrożenia i sposoby ich unikania podczas korzystania z Internetu

Dzień dobry!

Robisz zakupy czy pragniesz nawiązać kontakty z bliskimi – po przeczytaniu naszej broszurki korzystanie z Internetu stanie się łatwiejsze.

Dowiesz się jak unikać zasadzek cyberoszustów.

Poznasz zagrożenia związane z zakupami w sieci.

Nauczysz się jak bezpiecznie dokonywać płatności.

Dowiesz się jak się bronić przed zagrożeniami, jak rozpoznawać podejrzane wiadomości i chronić się przed kradzieżą danych.

Zostaniesz poinformowany jakie formy działania na psychikę są stosowane w sieci.

Rodzice, Dziadkowie, Bliscy uczniów Zespołu Szkolno – Przedszkolnego w Łobzowie

Internet to miejsce nieograniczonych możliwości. Szkoda byłoby z nich nie skorzystać ! Przedstawimy kilka informacji, które ułatwią Wam bezpieczne korzystanie z Internetu.

Bezpieczeństwo rodziców i dziadków w Internecie

Dlaczego zebraliśmy te informacje?

Chcemy pomóc naszym rodzicom i dziadkom, aby nie czuli się wykluczeni z życia społecznego. Dzisiaj coraz więcej spraw trzeba załatwiać przez Internet. Udowodnimy, że nie jest to trudne. Wystarczy tylko przestrzegać zasad, a będziemy bezpieczni.

Rodzice, Dziadkowie, Osoby Starsze – jakie wybierają formy korzystania z Internetu?

- Zakupy online
- Kontakty z bliskimi
- Załatwianie spraw urzędowych

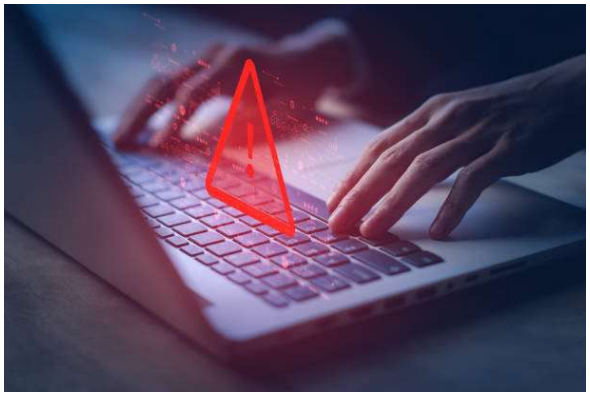
Kontakt z nami

Naszą broszurę możesz otrzymać od uczniów ZSP w Łobzowie.
Zostanie też umieszczona na stronie szkoły. Możesz też zatelefonować, a nasi uczniowie dostarczą Ci wersję papierową.

Telefon: 32 644 10 60
e-mail: splobzow@poczta.onet.pl

ZAGROŻENIA

Najważniejsze zasady bezpieczeństwa w mediach społecznościowych



Co robić, kiedy podejrzewamy, że konto zostało zaatakowane?

Gdzie zgłaszać podejrzenia włamań na konta w mediach społecznościowych lub innych serwisach internetowych?

Policja – Biuro do Walki z Cyberprzestępczością: cyber-kgp@policja.gov.pl Należy pamiętać, że w każdej wojewódzkiej komendzie Policji działa Wydział do Walki z Cyberprzestępczością.

NASK (CSIRT NASK) cert@cert.pl oraz https://incydent.cert.pl/

JAK SIĘ PRZED NIMI CHRONIĆ?

1. Utwórz silne hasło. Upewnij się, że nie korzystasz z żadnego ze swoich haseł na wielu kontach.
2. Ogranicz dostęp do konta. Uaktywnij dwuskładnikowe uwierzytelnianie na wszystkich swoich kontach.
3. Dodawaj do listy swoich znajomych wyłącznie osoby, które rzeczywiście znasz i którym ufasz.
4. Nie ufaj udostępnianym w serwisach aplikacjom.
5. Korzystaj tylko z oficjalnych aplikacji sieci społecznościowych Aplikacje pobieraj wyłącznie z oficjalnych sklepów — np. Google Play dla Android, App Store dla iOS i Microsoft Store dla Windows.
6. Dbaj o prywatność Praktycznie wszystkie serwisy społecznościowe posiadają rozwiązania w zakresie zwiększania prywatności – aktywuj je!
7. Używaj programu antywirusowego i funkcji bezpieczeństwa w przeglądarkach internetowych.

Postaraj się zalogować i sprawdzić dane dotyczące konta (adres e-mail i telefon), aby podjąć próbę sprawdzenia, kto ma dostęp do Twoich informacji. Natychmiast zmień hasło na nowe - silne i niepowtarzalne - i włącz uwierzytelnianie dwuskładnikowe. Sprawdź swoje konta w innych serwisach społecznościowych i poszukaj zaleceń, dotyczących czynności w przypadku ataku.

Wyłudzenia danych:

phishing - metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych do logowania, danych zawartych na karcie płatniczej, haseł, kodów PIN).

Ataki phishingowe polegają na przesłaniu krótkich wiadomości tekstowych, które pobudzają silne emocje, że np. ktoś nas okrada, dzieje się krzywda bliskim, szantaż, oskarżenie o popełnienie przestępstwa, blokada środków na koncie.

Nie klikaj w linki, nie otwieraj załączników od nieznanych nadawców. Zanim **klikniesz w nieznany, podejrzany link** korzystając z darmowych narzędzi UrlVoid, czy LinkScanner, możesz sprawdzić, czy pod odnośnikiem nie kryje się niebezpieczeństwo. 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.

Malware: (Infekuje urządzenia, działa na szkodę użytkownika (także straty finansowe); Może to być: załącznik lub odnośnik (link) w wiadomości e-mail, przejęta przez przestępców lub podstawiona, fałszywa strona, podstawione reklamy na zwykłych stronach

Stosuj aktualizacje, posiadaj oprogramowanie antywirusowe, regularne skanuj oprogramowanie antywirusowe, rób kopie zapasowe danych, posiadaj firewalla (działa jak zapora nie dopuszczająca szkodliwych elementów i ataków z zewnątrz).

Złośliwe oprogramowanie (tzw 'wirus') służy min. do przejmowania kontroli nad zainfekowanym systemem czy wykradania haseł, danych itd.)

Nie pobieraj treści z niezaufanych stron internetowych.
Zainstaluj antywirusa (może usuwać złośliwe programy, ostrzegać przed fałszywymi witrynami czy uprzedzać przed stronami zawierającym złośliwy kod) / firewalla. **Systematycznie sprawdzaj komputer na obecność wirusów. Używaj programów ze znanych, zaufanych źródeł.**
Aktualizuj oprogramowania i zmieniaj hasła dostępu do kont i profili w usługach cyfrowych.

Spam (niechciana poczta, może być to jedynie duża ilość irytujących wiadomości takich jak reklamy itp., jednakże często w tych pozornie nieszkodliwych treściach kryją się niebezpieczne szkodniki) oraz szkodliwe wiadomości na e-mailu.

Klikaj tylko w wiadomości e-mail, co do których masz pewność od kogo pochodzą, a jeśli już coś otworzysz, to dokładnie sprawdź autentyczność takiego e-maila. Sprawdź, czy link, w który klikasz na pewno przekierowuje na właściwą stronę banku, a nie jest zwykłym oszustwem.

Jeśli przez pomyłkę lub z ciekawości otworzymy zainfekowany załącznik, może to skutkować przedostaniem się do naszego komputera szkodliwego oprogramowania.

Wiadomości mogą na pierwszy rzut oka wyglądać jak np. wiadomość od naszego banku, z przekierowaniem na rzekomo oficjalną stronę banku (którą oczywiście nie jest), aby po zalogowaniu się na nią nieostrożnego internauty uzyskać jego dane do konta.

Przez nieostrożność możemy kliknąć np. w link 'do banku', który zamiast www.ing.pl będzie brzmiał www.iing.pl. Uważaj przy otwieraniu załączników, mogą zawierać wirusy, nawet w plikach pozornie wyglądających jak obrazki czy dokumenty tekstowe.

Oszustwo na dyrektora - atak BEC, czyli Business Email Compromise wykorzystuje phishing ukierunkowany na instytucje, przedsiębiorstwa i organizacje. Metoda oparta jest na socjotechnice stosowanej wobec pracownika firmy. Atakujący wywiera wpływ poprzez nakłonienie do szybkiego wykonania określonego zadania nałożonego przez „kierownictwo wyższego szczebla".

Nigdy nie otwieraj podejrzanych linków, załączników.
Otwieraj te, których się spodziewasz lub potwierdź u nadawcy (jeśli to znajomy, współpracownik), że to on wysłał tego maila. Zachowaj szczególną ostrożność podczas korzystania z osobistej skrzynki pocztowej korzystając ze sprzętu firmowego. Ściśle stosuj się do wewnętrznych procedur dotyczących płatności i zamówień.

<u>Najczęstsze metody oszustw wobec seniorów:</u>

Metoda na wnuczka – w sieci działa w podobny sposób jak w realnym życiu. Wystarczy, że ktoś włamie się na konto społecznościowe bliskiej osoby lub skorzysta z jej komunikatora, aby wyłudzić pieniądze. Wiadomości wysyłane przez oszustów mogą zawierać linki, które po kliknięciu przeniosą seniora na fałszywą stronę z płatnościami.

Metoda na kod czy też na znajomego – działa na podobnej zasadzie jak metoda na wnuczka. Osoba „znajoma" odzywa się do seniora i prosi o podanie np. danych karty kredytowej lub debetowej, tłumacząc jednocześnie, że pilnie musi zapłacić za zakupy, a właśnie nie ma przy sobie portfela.

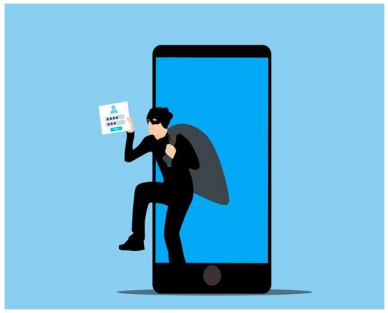
Nigdy nie otwieraj podejrzanych linków, załączników.
Otwieraj te, których się spodziewasz lub potwierdź u nadawcy (jeśli to znajomy, współpracownik), że to on wysłał tego maila. Zachowaj szczególną ostrożność podczas korzystania z osobistej skrzynki pocztowej korzystając ze sprzętu firmowego.
Używaj silnego hasła (najlepiej składające się z losowych znaków – np. manager haseł) i inne niż wykorzystywane w pozostałych serwisach. Pamiętaj, że informacją jest:
- tekst,
- zdjęcie lub film,
- charakterystyczne obiekty pozwalające na identyfikację Twojego miejsca przebywania lub Twoich bliskich,

Wykorzystywanie zaufania do instytucji – zdarza się, że oszuści podają się za ZUS, Urząd Skarbowy czy bank, aby wyłudzić wrażliwe informacje. Często wysyłają też wiadomości e-mailowe ze specjalnym linkiem, który po kliknięciu instaluje złośliwe oprogramowanie i pozwala przestępcom przejąć dane dostępowe do różnych serwisów.

Fałszywe zbiórki pieniędzy – na szczęście coraz większa liczba zbiórek jest weryfikowana, a osoby, które zbierają datki, muszą przejść dokładną kontrolę. Niestety jednak wciąż jeszcze zdarzają się sytuacje, w których organizatorzy nielegalnej kwesty próbują w ten sposób oszukać wrażliwych seniorów.

Zakupy w sieci – niedostarczenie towaru, fałszywe linki, kradzież danych z kart mpłatniczych

• polubione miejsca (jak również „meldowania") lub grupy, do których należysz Pamiętaj, że korzystając z serwisów społecznościowych łatwo można (również nieintencjonalnie)zdradzić poufne i wrażliwe dane osób trzecich, pracodawcy, kontrahenta. Skasuj swój profil w serwisie, z którego nie będziesz więcej korzystać. Jeśli padłeś ofiarą przestępstwa internetowego, nie kasuj żadnych danych, sporządź kopię całej korespondencji.



Nie korzystaj z publicznych sieci WI-FI; nie trać kontaktu ze swą kartą kredytową; podczas płatności sprawdź, czy przekierowanie jest na stronę banku; dokonuj płatności na bezpiecznych urządzeniach z oprogramowaniem antywirusowym; wybieraj bezpieczne metody płatności; sprawdź dane sprzedawcy; korzystaj z zabezpieczonych stron (symbol kłódki), w przeglądarce na początku powinien być HTTPS zamiast http.

https://www.gov.pl/web/baza-wiedzy/bezpieczni-w-sieci
https://glosseniora.pl/2023/10/03/bezpieczenstwo-seniorow-w-sieci-jak-unikac-oszustw-i-zagrozen-online/
https://cik.uke.gov.pl/news/bezpieczny-senior,307.html