Gdzie zgłaszać incydenty związane z bezpiezeństwem w sieci?

Do zespołu CERT Polska możesz zgłosić:

- podejrzane wiadomości e-mail/SMS, phishing
- próby oszustwa (np. fałszywe sklepy internetowe)
- złośliwe oprogramowanie
- nielegalne treści w internecie (zgłoszenie trafi do zespołu Dyżurnet.pl)
- błędy w aplikacjach internetowych lub oprogramowaniu
- wszelkie inne niepokojące Cię zdarzenia w sieci (np. próby nieuprawnionego logowania)
- złośliwą domenę, która służy do wyłudzania danych osobowych i środków finansowych.

Wszystkie próby kradzieży tożsamości, kradzieży środków finansowych, wymuszenia okupu i inne przestępstwa zgłoś również na policji.

ZGŁOŚ:
- poprzez formularz: https://incydent.cert.pl/
- lub bezpośrednio: cert@cert.pl

Każdy incydent możesz zgłosić anonimowo.

NASK Przestrzeń from facebook unicef dla każdego dziecka

Zgłaszaj fałszywe lub zhakowane konta!

Nie możesz zalogować się na konto? Z Twojego profilu wysyłane są wiadomości, których nie napisałaś/napisałeś? Prawdopodobnie Twoje konto zostało zhakowane czyli... ktoś się na nie włamał. Zgłoś taką sytuację administratorowi serwisu.

Jak zrobić to na Facebooku? Dowiedź się teraz!

Chroń się przed włamaniem.

Serwisy społecznościowe coraz częściej oferują możliwość uwierzytelniania dwuskładnikowego, które pomoże lepiej chronić Twoje konto. Jak to działa? To proste. Logując się na konto podajesz nie tylko hasło, ale również jednorazowy kod, który otrzymasz SMSem lub pobierzesz ze specjalnej aplikacji. Nawet jeśli cyberprzestępcy przechwycą Twoje hasło, nie zdołają dostać się na Twój profil.

Jak możesz ustawić uwierzytelnianie dwuskładnikowe na Facebooku? Sprawdź!

Co zrobić po ataku?

- Upewnij się, że powiadomienie o zagrożeniu wirusem (lub innym złośliwym oprogramowaniem) otrzymałeś faktycznie od swojego programu antywirusowego zastosuj się do jego zaleceń (może to być naprawa pliku, kwarantanna, albo zalecenie usunięcia).
- Jeśli antywirus nie może poradzić sobie z zagrożeniem, odłącz urządzenie od internetu i powtórnie zainstaluj system operacyjny. W przypadku smartfona, czy tabletu najbezpieczniejszy będzie również całkowity reset urządzenia. Pamiętaj, że przy okazji usuniesz wszystkie prywatne dane - to dlatego tak ważne jest regularnie tworzenie kopii zapasowej.
- Poproś o pomoc specjalistę (serwis). Pamiętaj, że czasami próba reanimowania urządzenia po ataku jest bardzo czasochłonna, a koszty z nią związane mogą przewyższać jego wartość. Zapytaj o to.

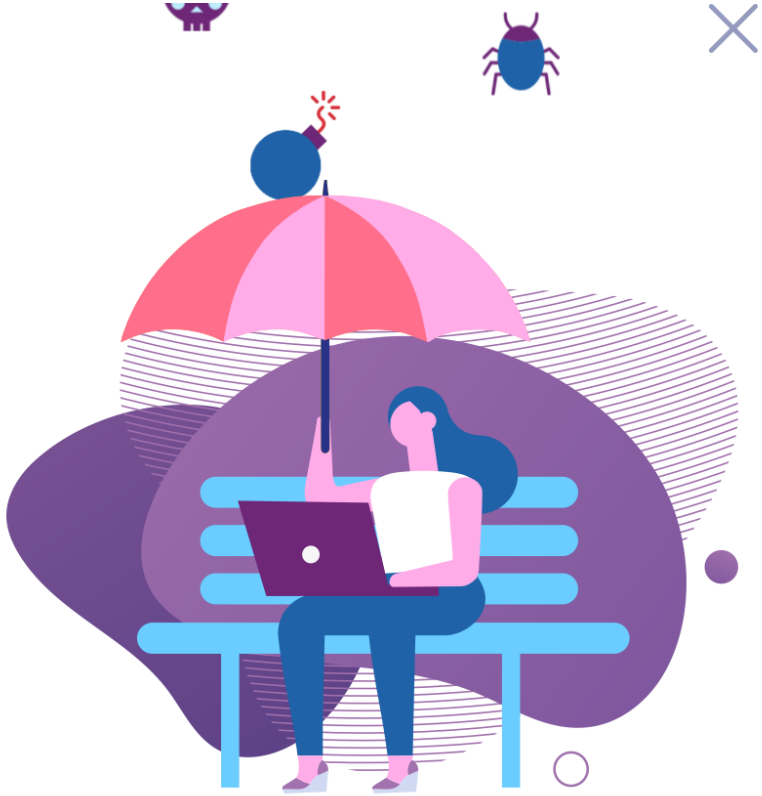
Zgłoś incydent

Dlaczego to takie ważne? Nie tylko Ty możesz być poszkodowany. Twoje urządzenie mogło posłużyć cyberprzestępcom do zaatakowania innych osób lub instytucji. Szybkie zgłoszenie pomoże zespołom reagowania na incydenty zatrzymać dalsze ataki.

Sposoby reagowania

Jeśli rozważnie poruszasz się w sieci i dbasz o aktualizacje, znacznie zmniejszasz ryzyko cyberataku. Jednak nawet przy zachowaniu ostrożności możesz paść ofiarą oszustów i hakerów w sieci.

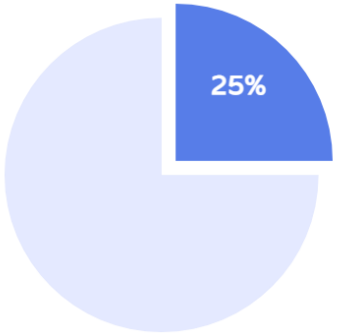
Czasami atak jest dla nas oczywisty - np. wtedy, kiedy otrzymujemy żądanie okupu, ale bywa też tak, że nie wiemy, że nasz komputer czy smartfon jest zainfekowany. Jak to rozpoznać? Co zrobić? Dowiesz się w dalszej części kursu.



Co powinno wzbudzić Twoją czujność?
Aby dowiedzieć się więcej, dopasuj hasło do odpowiedniego opisu.

Wyjątkowa okazja	Gigantyczny rabat tylko dzisiaj oraz ceny wielokrotnie niższe, niż w innych sklepach mają za zadanie wywołać poczucie presji i nakłonić Cię do szybkiego dokonania zakupu.
Tylko przelew	Jeśli jedyną opcją płatności jest dokonanie przelewu, istnieje duże prawdopodobieństwo, że zostaniesz oszukany. Nigdy nie przesyłaj też zdjęć karty kredytowej.
Sprawdzam	Sprawdź informacje o sprzedającym, wyszukaj nazwę sklepu i upewnij się, czy ktoś już nie zgłosił go jako fałszywego sklepu..
Chciałbym zajrzeć na Twój profil	Jeśli sprzedający/serwis prosi Cię o zalogowanie do Facebooka, banku lub w innym miejscu, klikanie w podejrzane linki, zainstalowanie czegokolwiek – wycofaj się.
Komu płacę?	Dokonując płatności online sprawdź, czy adresatem jest rzeczywiście osoba/firma, której chcesz zapłacić. Cyberprzestępcy próbują wyłudzić legalne płatności za pośrednictwem fałszywych sklepów.
Witryna zrobiona „na kolanie”	Zwróć uwagę na wszystkie niedociągnięcia i niespójności - błędy, słabej jakości zdjęcia, brak niektórych elementów (np. regulaminu, sposobu dokonywania zwrotów).

Bezpieczne zakupy w sieci



Prawie 25% nastolatków deklaruje, że jednym z najczęstszych sposobów używania internetu jest dla nich… korzystanie ze sklepów internetowych i serwisów aukcyjnych.

Zakupy online stają się coraz bardziej popularne, a zarówno nieuczciwi sprzedawcy, jak i cyberprzestępcy coraz częściej próbują wykorzystać nieuwagę kupujących. Prawie co dziesiąty nastolatek został oszukany podczas transakcji w sieci.

Dowiedz się więcej o bezpiecznych zakupach w sieci:
Jak nie dać się złapać w sieci nieuczciwych sprzedawców. Poradnik zespołu CERT Polska, (2019) .

Pozbywasz się starego telefonu - usuń dane

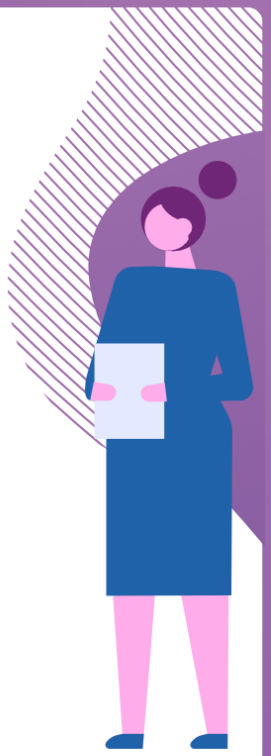
Smartfon, tablet czy smartwatch przechowują bardzo dużo informacji na Twój temat.

Pamiętaj, aby przed pozbyciem się takiego urządzenia wykasować znajdujące się na nim dane. Najprostszym sposobem będzie przywrócenie ustawień fabrycznych urządzenia (znajdziesz taką opcję w ustawieniach). Nie zapominaj, że Twoje dane nadal zapisane są na karcie SIM - jeśli nie planujesz używać jej w nowym urządzeniu, zniszcz ją.

Podsumowując

Pamiętaj, że możesz zrobić wiele, żeby zabezpieczyć się przed cyberatakiem.

- Nie zapominaj, że nie tylko komputer czy laptop wymagają aktualizacji. Twój smartfon również.
- Używaj aktualnej wersji programu antywirusowego.
- Rób aktualizacje systemu i aplikacji.
- Pobieraj aplikacje tylko z zaufanych źródeł.
- Ustawiaj bezpieczne hasła. Nie stosuj tego samego hasła w wielu miejscach.
- Nie loguj się na konta bankowe lub służbowe używając publicznie dostępnych komputerów (np. w bibliotece, hotelu) oraz korzystając z publicznie dostępnej sieci Wi-Fi. Używaj tylko własnego sprzętu i zabezpieczonego hotspotu.
- Nie podłączaj do urządzenia niezaufanych nośników pamięci (zawsze skanuj nośniki pamięci przed otworzeniem na komputerze/laptopie).
- Twórz regularnie kopię zapasową danych.
- Usuwaj dane z urządzeń oraz aplikacje, których już nie używasz.



Gry online

Średnio co dwunasty nastolatek doświadczył kradzieży dóbr wirtualnych czyli np. cennych przedmiotów, zgromadzonych punktów, a prawie co dziesiąty oszustwa przy transakcji online. To wszystko może wydarzyć się przy okazji grania w sieci. A to nie wszystkie zagrożenia.

Należy zwrócić na następujące kwestie:

Gry online

Średnio co dwunasty nastolatek doświadczył kradzieży dóbr wirtualnych czyli np. cennych przedmiotów, zgromadzonych punktów, a prawie co dziesiąty oszustwa przy transakcji online. To wszystko może wydarzyć się przy okazji grania w sieci. A to nie wszystkie zagrożenia.

Należy zwrócić na następujące kwestie:

Gry online

Średnio co dwunasty nastolatek doświadczył kradzieży dóbr wirtualnych czyli np. cennych przedmiotów, zgromadzonych punktów, a prawie co dziesiąty oszustwa przy transakcji online. To wszystko może wydarzyć się przy okazji grania w sieci. A to nie wszystkie zagrożenia.

Należy zwrócić na następujące kwestie:

Sklepy dla graczy. Warto uważać podczas wymiany wirtualnych dóbr i sprawdzać opinie o sprzedających/ kupujących. Tu również działają oszuści, a nierozważna transakcja może kosztować gracza utratę wirtualnego, często unikatowego, majątku.

Cheaty. Dodatki, które mają ułatwić grę oraz strony, które je oferują, poza tym, że są nieuczciwym zagraniem, często infekowane są złośliwym oprogramowaniem. Nie warto iść na skróty.

Bezpieczne instalowanie aplikacji mobilnych

Aplikacje również mogą posłużyć cyberprzestępcom do zainfekowania urządzenia. Jak utrzymać smartfon z dala od złośliwych aplikacji?

- Pobieraj aplikacje tylko ze sprawdzonych i zaufanych źródeł.
- Sprawdź opinie i statystyki pobierania. Szukaj rozbieżności. Świetnie oceniona aplikacja i bardzo mało pobrań? Może być fałszywa.
- Przyjrzyj się uprawnieniom aplikacji. Sprawdź, do jakich elementów aplikacja potrzebuje dostępu, aby działać prawidłowo. Zastanów się, czy naprawdę ich potrzebuje. Jeśli cokolwiek Cię zaniepokoi, zrezygnuj z instalacji.
- Wyszukaj nazwę aplikacji. Wpisz w wyszukiwarkę nazwę ze słowami „opinie”, „oszustwo” i dowiedz się, czy ktoś nie ostrzega przed tą konkretną aplikacją.

A później?

- Korzystaj z aktualizacji dostępnych dla aplikacji.
- Usuń aplikacje, z których już nie korzystasz.

Jak zabezpieczyć się przed cyberatakami?

Pamiętaj, że możesz zrobić wiele, aby nie narazić się na atak cyberprzestępców. Co najważniejsze, nie wymaga to od Ciebie szczególnych starań, ani specjalistycznej wiedzy.

Hasła

Aktualizacje

Kopie zapasowe

Zdrowy rozsądek

Hasła

Silne i unikatowe hasło to jedna z barier zapobiegających cyberatakowi.

1. Twórz silne hasła, czyli takie, które nie będą łatwe do odgadnięcia przez inną osobę albo automat.
2. Używaj innego hasła do każdego z urządzeń, kont w serwisach i aplikacji.
3. Pamiętaj o każdorazowym wylogowaniu się.
4. Jeśli Twoje konto zostanie zhakowane, zmień wszystkie hasła.
5. Jeśli masz taką możliwość, korzystaj z uwierzytelniania dwuskładnikowego, ponieważ cyberprzestępcy cały czas udoskonalają technologie ułatwiające łamanie haseł.

Aktualizacje aplikacji i urządzeń

Upewnij się, że wszystkie urządzenia, które podłączasz do sieci (komputer, urządzenia mobilne, aplikacje, ale też Smart TV, konsole do gier czy routery) używają najnowszej wersji oprogramowania. Cyberprzestępcy nieustannie szukają luk w oprogramowaniu, aby włamać się na urządzenie, a twórcy technologii starają się temu zapobiec, łatając te luki. Aktualizacja jest właśnie taką „łatką" nałożoną na lukę w systemie.

Większość urządzeń sama przypomina Ci o dostępnych nowych aktualizacjach, nie odkładaj zainstalowania ich na później.

Kopie zapasowe

Niezależnie od tego, jak wiele środków ostrożności podejmiesz, Twój komputer czy smartfon może zostać zaatakowany. Często jedynym sposobem na pozbycie się złośliwego oprogramowania jest całkowite usunięcie zainfekowanego systemu i zainstalowanie go ponownie na urządzeniu.

Jeśli przez cyberatak nie możesz odzyskać dostępu do prywatnych plików przechowywanych na urządzeniu, może się zdarzyć, że jedynym rozwiązaniem będzie odtworzenie ich z kopii zapasowej.

Regularnie twórz kopie zapasowe wszystkich ważnych danych.

Większość systemów operacyjnych umożliwia ustawienie automatycznego tworzenia kopii zapasowych - zazwyczaj są one umieszczane w chmurze.

Możesz również regularnie tworzyć kopię danych na zewnętrznym nośniku, np. dysku zewnętrznym.

I najważniejsza ochrona przed cyberatakiem - zdrowy rozsądek!

Włącz czujność:

- nie ufaj wyjątkowym okazjom
- weryfikuj u źródła (w banku, firmie kurierskiej, sklepie internetowym, itp.) wiadomości, które wymagają od Ciebie natychmiastowych działań
- nie klikaj w przesłane w mailach/SMSach linki, nie instaluj dodatkowych programów/ aplikacji
- sprawdzaj podejrzane wiadomości od Twoich rzekomych znajomych kontaktując się z nimi bezpośrednio
- nie poddawaj się presji - nie podejmuj działania w emocjach

Rozmawiaj z uczniami o socjotechnice, ponieważ większość ataków jest skuteczna dlatego, że sami otwieramy przed cyberprzestępcami drzwi do naszych danych.