„ABC CYBERBEZPIECZEŃSTWA”
ulotka promocyjna dla dzieci, młodzieży i rodziców w ramach Dnia Bezpiecznego Internetu 2024 w Zespole Szkolno-Przedszkolnym w Łysej Górze

ADWARE - natarczywe reklamy, przede wszystkim w formie bannerów lub wyskakujących okien przeglądarki internetowej– niechciane oprogramowanie, które podszywa się pod pozornie bezpieczne aplikacje, aby skłonić użytkowników do zainstalowania ich na swoich urządzeniach (telefonach, komputerach, tabletach). Bywa, że takie programy występują w pakiecie z innym bezpłatnym oprogramowaniem. Złośliwe oprogramowanie typu adware może być niebezpieczne – zdarza się, że automatycznie przekierowuje na określone strony internetowe, a także łączy się np. z programami szpiegującymi (spyware) czy umożliwiającymi włamania do systemów informatycznych (rootkit).
Jak chronić się przed adware? Korzystajcie tylko z wiarygodnych źródeł. Korzystajcie też z antywirusa. Jeśli zauważycie coś niepokojącego, odinstalujcie nową aplikację, którą podejrzewacie o to, że jest powiązana z programem typu adware.

BACKDOOR - To pojęcie możemy przetłumaczyć jako „tylne drzwi” lub „furtka”, to umyślnie pozostawiona luka w zabezpieczeniach systemu komputerowego. Celem tego działania jest późniejsze wykorzystanie „szczeliny” w oprogramowaniu do bardzo niebezpiecznych działań, takich jak np. przejęcie kontroli nad zainfekowanym systemem. Backdoor może zostać pozostawiony przez złośliwe oprogramowanie (malware), cyberprzestępcę, ale też umyślnie stworzony przez autora danego programu. Niestety „tylne drzwi” mogą być ogromnym zagrożeniem, dlatego zawsze trzeba pamiętać o zasadach bezpiecznego korzystania z urządzeń cyfrowych, w tym o aktualizacji oprogramowania i programu antywirusowego czy rozważnym instalowaniu aplikacji i innych narzędzi.

Bomba logiczna - To rodzaj złośliwego oprogramowania (malware), które aktywuje się po spełnieniu określonych warunków. Tykająca bomba eksplodująca w najmniej oczekiwanym momencie? „Detonacja” może nastąpić np. w określonym dniu tygodnia lub o danej godzinie (bomba czasowa), po otwarciu przeglądarki, zalogowaniu się konkretnego użytkownika, otwarciu lub usunięciu pliku czy uruchomieniu programu. W wyniku jej działania możecie stracić swoje pliki, a nawet dane z dysku twardego. Zablokowanie dostępu do określonych programów lub aplikacji to również częste skutki uruchomienia szkodliwego kodu. Ponadto przestępcy mogą wykorzystać Wasz adres e-mail do przeprowadzenia kampanii spamowych (spam).
Jak się bronić przed tego typu atakiem? Jak zawsze korzystajcie z programów antywirusowych, dbajcie o regularne aktualizacje, pobierajcie oprogramowanie tylko ze sprawdzonych źródeł oraz uważajcie na ataki phishingowe.

BOTNET - czyli grupa komputerów-zombie zainfekowanych szkodliwym oprogramowaniem, umożliwiających cyberprzestępcy przejmowanie kontroli nad wieloma (a czasem nawet nad setkami lub tysiącami!) „zarażonymi” komputerami i wykorzystywanie ich np. do wykradania danych osobowych, rozsyłania spamu lub wirusów czy przeprowadzania ataków DDoS. Ponadto wszystkie te operacje dzieją się bez wiedzy i zgody właścicieli sprzętów, którzy są nieświadomi, do czego wykorzystuje się ich komputery.

BROWSER HIJACKER - przejmuje kontrolę nad przeglądarką internetową, zarządzając nią bez udziału użytkownika. W efekcie może się nagle okazać, że Wasza strona główna została zmieniona lub otwierają się witryny, których nie zamierzaliście odwiedzać – najczęściej przeładowane reklamami czy nieodpowiednimi treściami. W ten sposób przestępcy czerpią zyski z liczby wejść na daną stronę. Co więcej, „porywacz przeglądarek” uniemożliwia dostanie się na platformy z oprogramowaniem antywirusowym czy antyszpiegowskim. Takie działania znacznie utrudniają korzystanie z internetu, a nawet bywają bardzo niebezpieczne. Oprócz problemów z przeglądaniem sieci browser hijacker może bowiem zawierać oprogramowanie szpiegujące, np. keyloggery.

CYFROWY ŚLAD - Nasze dane trafiają do baz danych i chmur obliczeniowych, a tam… zaczynają żyć własnym życiem. Swój cyfrowy ślad możemy zostawiać celowo – gdy wysyłamy e-maile, komentujemy posty w mediach społecznościowych, publikujemy zdjęcia czy filmy. Bierne ślady to m. in. informacja o systemie operacyjnym, adresie IP, używanej przeglądarce internetowej, ale też dane geolokalizacyjne czy godzina i data wykonania zdjęcia dodanego do posta w social mediach. Nawet jeśli wydaje nam się, że pozostajemy anonimowi, udostępniamy informacje o swoich kliknięciach, które mogą być analizowane, rejestrowane i przechowywane.
Czy można zminimalizować swój cyfrowy ślad? Bądźcie uważni w mediach społecznościowych – dostosujcie ustawienia prywatności i rozważnie dzielcie się treściami w internecie. Dodatkowo używajcie trybu prywatnego (incognito, In Private) w przeglądarkach, dzięki czemu uchronicie się przed zapisywaniem Waszej historii przeglądania, danych w formularzach czy tzw. ciasteczek. Pamiętajcie też o regularnych porządkach – pozbywajcie się nieużywanych kont czy adresów e-mail oraz sprawdźcie, czy aplikacje, z których korzystacie, nie mają dostępu do zbyt wielu Waszych danych.

DDOS (DISTRIBUTED DENIAL OF SERVICE) ATAKI TYPU DDOS (Z ANG. ROZPROSZONA ODMOWA USŁUGI) - ich celem jest zajęcie wszystkich dostępnych i wolnych zasobów komputera. Takie działanie cyberprzestępców ma uniemożliwić korzystanie z urządzenia i dostępnych na nim zasobów, a co za tym idzie – blokować funkcjonowanie usługi online (np. strony internetowej czy poczty e-mail znajdującej się na hostingu). Ataki DDoS przeprowadzane są z wielu miejsc jednocześnie, czyli z wielu komputerów, nad którymi kontrolę przejęło specjalne oprogramowanie, takie jak boty czy trojany.
Zastanawiacie się, jak chronić się przed atakami tego typu? Najlepszą obroną jest regularne aktualizowanie programu antywirusowego. Można korzystać też ze specjalnego oprogramowania, które filtruje ruch sieciowy noszący znamiona ataku DDoS.

„ABC CYBERBEZPIECZEŃSTWA”
ulotka promocyjna dla dzieci, młodzieży i rodziców w ramach Dnia Bezpiecznego Internetu 2024 w Zespole Szkolno-Przedszkolnym w Łysej Górze

DEEPFAKE - sfabrykowane nagrania, stworzone przy użyciu prawdziwych próbek głosu, wideo i zdjęć. Film z udziałem znanego polityka lub celebryty zawierający nieprawdziwe, niewiarygodne informacje? Jest to technika obróbki obrazu, która korzysta z rozwiązań sztucznej inteligencji (SI): algorytm na podstawie realnych danych tworzy łudząco prawdopodobny, jednak zmanipulowany materiał. Co więcej, takie filmy działają zwykle na niekorzyść rzekomo występujących w nich osób, mogą być zatem wykorzystywane np. jako element walki politycznej.

DOXING - Dokładnie oznacza śledzenie i gromadzenie informacji w sieci, na temat określonej osoby lub organizacji w celu analizy zebranych danych, a następnie ich upublicznienia. Doxer szuka wstydliwych zdjęć lub filmików, kontrowersyjnych wypowiedzi, danych osobowych i wrażliwych. W tym celu wciela się w cyfrowego detektywa, który legalnie uzyskuje informacje z sieci, ale też w cyberprzestępcę wykorzystującego oprogramowanie szpiegujące bądź socjotechnikę, by zmanipulować ofiarę i uzyskać interesujące go dane.
Zanim wrzucicie coś do sieci – zastanówcie się, jak to wpłynie na Wasz wizerunek. Warto też zadbać o swoją prywatność w internecie: na portalach społecznościowych ustawiajcie profil prywatny zamiast publicznego, nie publikujcie zdjęć, z których można pozyskać istotne dane – biletów lotniczych, dokumentów tożsamości czy kart kredytowych (nawet ich fragmentów).

EXPLOIT - to program wykorzystujący istniejące błędy w oprogramowaniu. Cyberprzestępca poprzez lukę przejmuje kontrolę nad urządzeniem lub zmusza je do wykonania żądanej przez niego operacji. Aby uchronić się przed konsekwencjami zainfekowania exploit, należy m. in. korzystać z legalnych programów i oprogramowania antywirusowego, warto też pamiętać, by nie klikać w podejrzane linki.

FAŁSZYWE DOMENY- tworzenie stron internetowych podszywających się pod znane podmioty, firmy i instytucje. Co je odróżnia? Zazwyczaj niewiele – może to być błąd w nazwie strony, np. cyfra „0” zamiast litery „O”. Bądźcie czujni, bardzo łatwo jest wpaść w sidła przestępców i przez nieuwagę zalogować się w oknie fałszywej strony banku, bramce płatności internetowej czy witrynie instytucji łudząco podobnej do tej prawdziwej. Dlatego zawsze zwracajcie szczególną uwagę na to, w co klikacie i gdzie wpisujecie swoje hasła i loginy! Jeśli traficie na taką fałszywą stronę, warto to zgłosić do CERT Polska. Wystarczy wypełnić formularz dostępny na CERT.PL – zgłoś incydent.

HAPPY SLAPPING - Rozśmieszyć odbiorców i oczywiście zwiększyć statystyki „kliknięć” – taki cel mają twórcy „zabawnej przemocy”, to forma cyberprzemocy, której powinniśmy się stanowczo przeciwstawiać. Szczególnie że nagrania tego typu bardzo szybko rozprzestrzeniają się w sieci, a skutki agresji w internecie mogą być długofalowe i wiązać się z poważnymi problemami psychosomatycznymi, depresją, lękiem oraz obniżonym poczuciem wartości ofiary.

JAVASCRIPT INJECTION - To forma ataku na witrynę internetową, która polega na ulokowaniu (ang. injection – wstrzyknięciu) w jej treści kodu JavaScript uruchamianego po stronie użytkownika. Atakujący stronę oszust zyskuje dzięki temu wiele możliwości – jest w stanie modyfikować projekt witryny, uzyskiwać z niej informacje i manipulować parametrami (z wykorzystaniem plików cookie). Efektem „wstrzyknięcia” kodu JavaScript może być np. wyciek poufnych informacji, istotna zmiana parametrów lub włamanie do kont użytkowników.

KEYLOGGER - szkodliwe oprogramowanie monitoruje Waszą aktywność na urządzeniu. Śledzi ruch ofiary na klawiaturze i przekazuje dane osobom trzecim, może też przechwytywać zrzuty ekranu, dźwięk z mikrofonu, a także rejestrować ruch kursora myszki. Tym sposobem w niepowołane ręce wpadają poufne informacje: dane logowania do bankowości elektronicznej, poczty e-mail czy serwisów społecznościowych. Spowolnione działanie sprzętu, zawieszanie się komputera czy pojawienie się na dysku folderu ze zrzutami ekranu, którego sami nie stworzyliście – te sygnały powinny Was zaniepokoić!
Aby uchronić się przed zainfekowaniem, pamiętajcie o aktualizacjach – także przeglądarki internetowej i oprogramowania antywirusowego. Podczas logowania stosujcie uwierzytelnianie dwuskładnikowe. Nie klikajcie w podejrzane linki, a jeśli to możliwe – korzystajcie z wirtualnej klawiatury. To aplikacja, która umożliwia wpisywanie loginów i haseł bez użycia fizycznej klawiatury.

KOŃ TROJAŃSKI (TROJAN) - To rodzaj szkodliwego oprogramowania, podszywają się pod przydatne aplikacje bądź programy, sprawiając wrażenie użytecznych. W rzeczywistości wykonują wiele szkodliwych działań: instalują backdoor czy oprogramowanie szpiegujące (spyware) lub szyfrujące dane na komputerze ofiary, tak by nie miała do nich dostępu (ransomware). Szkodliwe oprogramowanie ukrywa się najczęściej w darmowych aplikacjach pochodzących z nieznanych źródeł, grach, a nawet w cyfrowych kartkach z życzeniami. Konia trojańskiego możecie też pobrać wraz z kliknięciem w baner reklamowy lub z zainfekowanym załącznikiem, np. przesłanym w poczcie e-mail. Pamiętajcie, przed szkodliwym oprogramowaniem ochroni Was przede wszystkim zdrowy rozsądek – nie otwierajcie e-maili od nieznanych osób, a już na pewno nie klikajcie w podejrzane linki. Ponadto pobierajcie aplikacje i pliki tylko z zaufanych źródeł. Warto też korzystać z zapory sieciowej firewall, która monitoruje przychodzące i wychodzące dane, a także z dobrego oprogramowania antywirusowego

KRADZIEŻ DANYCH - kradzież wirtualna cyberprzestępcy czyhają szczególnie na Wasze dane uwierzytelniające do bankowości elektronicznej, poczty e-mail, sklepów online, portali społecznościowych. Jeśli wejdą w ich posiadanie – stracicie nie tylko poczucie bezpieczeństwa, ale też posiadane środki na koncie. Przestępcy stosują różne metody, by zdobyć poufne informacje. Rozsyłają e-maile (phishing), SMS-y (smishing) albo dzwonią (vishing), podszywając się pod znane instytucje: urzędy, banki, firmy kurierskie. Grożą np. utratą dostępu do

„ABC CYBERBEZPIECZEŃSTWA”
ulotka promocyjna dla dzieci, młodzieży i rodziców w ramach Dnia Bezpiecznego Internetu 2024 w Zespole Szkolno-Przedszkolnym w Łysej Górze

internetowych usług, wymuszając na odbiorcy określone działanie – zazwyczaj nalegają na podanie loginów i haseł. Jeśli zauważyliście podejrzane domeny internetowe służące do wyłudzeń danych i środków finansowych, koniecznie zgłoście to do CERT Polska. Wystarczy wypełnić formularz online. A może przyszedł do Was dziwny SMS np. informujący o konieczności dopłaty do paczki? Prześlijcie tę wiadomość dalej – do CSIRT NASK: 799 448 084. Każde zgłoszenie może pomóc innym ustrzec się przed kradzieżą danych!

KRADZIEŻ TOŻSAMOŚCI - Wyobraźcie sobie, że dostajecie wezwanie do zapłaty za niezamawiane usługi, towary lub, co gorsza, monit o zaległych ratach kredytu, o którym nie mieliście pojęcia. Może się tak stać, jeśli Wasze dane osobowe – PESEL lub nr dowodu osobistego – wpadną w ręce cyberprzestępców. Złodzieje mogą zainfekować Wasz komputer wirusami lub przesłać e-mail z próbą wyłudzenia poufnych informacji. Źródłem cyberataku może być np. widoczny na opublikowanym przez Was zdjęciu dokument tożsamości czy fragment numeru karty kredytowej.
Jeśli padliście ofiarą kradzieży tożsamości, niezwłocznie powiadomcie o tym fakcie policję. Koniecznie poinformujcie też bank o podejrzanych transakcjach czy ewentualnych wnioskach kredytowych złożonych w Waszym imieniu.

KRUEGERWARE (KRUEGERAPPS)- Kruegerware zaliczany jest do niebezpiecznego oprogramowania typu malware (niszczącego zawartość komputera) i spyware (szpiegującego), trudno jest się go pozbyć, ponieważ może się odtworzyć nawet po usunięciu z komputera! Dzieje się tak np. przy wykorzystaniu mechanizmu odzyskiwania systemu Windows.
Jak się ustrzec przed tym zagrożeniem? Regularne aktualizacje systemu operacyjnego i programów na Waszym urządzeniu, a także korzystanie z oprogramowania antywirusowego – to podstawa. Jak zawsze pamiętajcie też o zachowaniu ostrożności podczas korzystania z sieci i urządzeń cyfrowych. Zanim klikniecie w link przesłany w e-mailu lub pobierzecie pliki z sieci – zastanówcie się dwa razy.

LIKEJACKING- Bywa, że „polubienia” wykorzystywane są przez cyberoszustów, którzy chcą zwiększyć oglądalność wybranych profili, aby otrzymywać korzyści z umieszczonych tam reklam. Próbują w tym celu zainteresować jak największą liczbę internautów szokującą wiadomością lub bardzo atrakcyjnym materiałem. Ci, którzy połkną haczyk, zostają przekierowani na stronę, gdzie rzekomo znajdą szczegółowe informacje. Zobaczą jednak nie zawartość, której się spodziewają, ale spreparowaną stronę z niewidoczną ramką, aktywującą się razem z kliknięciem. Efektem jest zmiana ustawień konta użytkownika. Co się stanie, gdy klikniecie w jakikolwiek przycisk lub obrazek na tej stronie? Wasz profil w mediach społecznościowych zostanie zainfekowany. Konto może stać się widoczne dla wszystkich (a więc dojdzie do zmiany ustawień prywatności), na tablicy pojawi się post o tym, że lubicie fałszywą stronę, a do Waszych znajomych trafi spam. Co więcej – pechowe kliknięcie może uruchomić instalację aplikacji, która będzie próbować wyłudzać pieniądze, pobierać inne szkodliwe oprogramowanie i wciąż rozprzestrzeniać się wśród osób z Waszej listy znajomych.
Przede wszystkim nie możecie bezrefleksyjnie klikać we wszystkie linki. Uważajcie też na wszystkie sensacyjne informacje, które widzicie w swoich mediach społecznościowych.

MALWARE (ZŁOŚLIWE OPROGRAMOWANIE) - to złośliwe oprogramowanie, mogące przysporzyć nie lada kłopotów, oznacza programy komputerowe, których celem jest wykonywanie szkodliwych działań, np. przejęcie kontroli nad urządzeniem ofiary czy kradzież danych, haseł bądź plików. Przykładami malware są m. in. wirusy, trojany, rootkit, oprogramowanie szyfrujące, robaki, keyloggery. Złośliwe oprogramowanie może zaatakować niemal każde Wasze urządzenie – smartfony, komputery, kamery, pendrive, a nawet inteligentne urządzenia domowe, takie jak wideodomofony, sprzęt RTV – telewizory, a nawet AGD – lodówki, pralki.
Aby chronić się przed malware, powinniście pamiętać o kilku ważnych zasadach, m. in. bieżącej aktualizacji oprogramowania i antywirusa, pobieraniu aplikacji i programów tylko z wiarygodnych źródeł, nieklikaniu w podejrzane linki i załączniki (np. otrzymane w e-mailu, SMS-ie), a także regularnym tworzeniu kopii zapasowych.

NARUSZENIA PRYWATNOŚCI - Każdy ma prawo do prywatności i ochrony danych osobowych, takich jak: imię i nazwisko, data urodzenia, adres e-mail, numer PESEL, czy wrażliwych informacji, np. wyników badań. Naruszenia prywatności to sytuacje, w których ktoś wykorzystuje cudzy wizerunek lub dane osobowe w celu wyrządzenia krzywdy osobistej bądź majątkowej. Przykładem takiego działania jest kradzież tożsamości, czyli przejęcie konta społecznościowego i podszywanie się pod jego właściciela. Przestępcy wykorzystują złośliwe oprogramowanie (malware), by zainfekować cudzy sprzęt i wykraść cenne informacje. Ponadto stosują phishing, wyłudzając w ten sposób wartościowe dane (hasła logowania do serwisów społecznościowych czy bankowości elektronicznej). Jeśli rejestrujecie się na nowej platformie lub w aplikacji, czytajcie politykę prywatności. Ponadto nie klikajcie w podejrzane linki, stosujcie silne i bezpieczne hasła, zmieńcie opcje prywatności w ustawieniach przeglądarki lub włączcie tryb incognito.

PASSWORD SPRAYING -To atak polegający na wykorzystaniu przez cyberprzestępców popularnych haseł w celu uzyskania dostępu do Waszych kont e-mailowych, założonych w bankowości elektronicznej czy sklepach online. Przede wszystkim zadbajcie o odpowiednie zabezpieczenie cyfrowych danych. Ostatnie rekomendacje CERT Polska w zakresie tworzenia silnych haseł zawierają np. zalecenie, by szyfry miały minimum 12 znaków i były łatwe do zapamiętania dla nas, ale trudne do odgadnięcia przez potencjalnych przestępców. Pamiętajcie też o stosowaniu uwierzytelniania dwuskładnikowego. Dodatkowy kod przesłany SMS-em czy za pośrednictwem aplikacji lub zabezpieczenie biometryczne sprawią, że Wasze dane będą bardzo trudne do przejęcia przez cyberprzestępców.

„ABC CYBERBEZPIECZEŃSTWA”
ulotka promocyjna dla dzieci, młodzieży i rodziców w ramach Dnia Bezpiecznego Internetu 2024 w Zespole Szkolno-Przedszkolnym w Łysej Górze

PHARMING - forma oszustwa polegająca na tworzeniu fałszywych stron internetowych, które podszywają się pod znane, bezpieczne witryny, i gromadzeniu w ten sposób poufnych danych. Użytkownicy korzystający ze stron bankowości elektronicznej są przekierowywani na łudząco podobne, podszywające się pod nie strony, które instalują na urządzeniach złośliwe oprogramowanie wykradające dane osobowe, takie jak dane kont bankowych czy hasła. Ustrzec się przed pharmingiem pomoże Wam stosowanie dobrze znanych zasad cyberhigieny: instalowanie i bieżące aktualizowanie programu antywirusowego, zwracanie uwagi na adres strony internetowej (sprawdzanie, czy nie ma w nim błędów, czy połączenie jest szyfrowane), a także nieotwieranie podejrzanych e-maili. Warto również włączyć uwierzytelnianie dwuskładnikowe oraz autoryzację transakcji w aplikacji banku. Pamiętajcie, że wszelkie oszustwa internetowe, w tym wyłudzenia danych i środków finansowych, możecie zgłaszać do zespołu CERT Polska za pośrednictwem specjalnego formularza.

PHISHING - Celem takich działań jest wyłudzenie poufnych danych – najczęściej logowania do serwisów społecznościowych lub bankowości elektronicznej. Podczas wirtualnego ataku oszust stara się wprowadzić nas w błąd i przekonać do wykonania określonej czynności: otwarcia zainfekowanego załącznika, kliknięcia w złośliwy link lub zalogowania się w oknie fałszywej strony (np. bramki do płatności elektronicznych). Aby osiągnąć swój cel, próbuje skontaktować się z ofiarą, wykorzystując sfabrykowane e-maile, SMS-y (vishing), wiadomości na komunikatorach i portalach społecznościowych. Do oszustwa może też dojść za pośrednictwem rozmowy telefonicznej (spoofing), podczas której przestępca podszywa się pod pracowników instytucji zaufania publicznego lub innego użytkownika. Najważniejsze są ostrożność i rozsądne podejście do otrzymywanych wiadomości. Pamiętajcie, że oszuści mogą podszywać się pod Waszych znajomych, zaufane instytucje czy firmy, z których usług korzystacie na co dzień. Waszą podejrzliwość powinna wzbudzić m. in. treść nakłaniająca do szybkiego i nieprzemyślanego działania lub udostępnienia wrażliwych danych, gdyż w przeciwnym wypadku wydarzy się coś złego (np. konto zostanie zablokowane) lub stracicie niepowtarzalną okazję

QUISHING - To forma phishingu, która wykorzystuje już nie linki przesyłane w e-mailach, ale odpowiednio spreparowane kody QR (ang. Quick Response, czyli szybka odpowiedź). W przypadku quishingu po zeskanowaniu takiego kodu, rzekomo prowadzącego do e-płatności lub odbioru nagrody, pobieramy zainfekowany plik lub trafiamy na fałszywą stronę banku czy innej instytucji. Uwaga! Z takimi kodami możecie mieć do czynienia nie tylko w e-mailach czy na stronach internetowych, ale też np. na przystankach komunikacji miejskiej, w klubach, restauracjach czy nawet na ubraniach! Tak jak w przypadku innych internetowych oszustw, przed quishingiem ochroni nas przede wszystkim zasada ograniczonego zaufania.

RANSOMWARE - To rodzaj złośliwego oprogramowania, którego zadaniem jest zaszyfrowanie danych na komputerze ofiary, tak by nie miała do nich dostępu. Atak ma najczęściej na celu wyłudzenie pieniędzy w zamian za odblokowanie systemu. Coraz częściej pojawiają się przypadki, kiedy to atakujący nie tylko szyfrują dane, ale także wykradają je, by następnie szantażować ofiarę, grożąc ich ujawnieniem lub poinformowaniem innych o ataku, np. partnerów biznesowych, instytucji współpracujących czy opinii publicznej w przypadku niezapłacenia okupu. Wystarczy, że otworzycie zainfekowany załącznik w e-mailu, zainstalujecie aplikację lub program pochodzący z nieznanego źródła czy klikniecie w natarczywą reklamę.
Jak zabezpieczyć się przed atakiem? Na bieżąco aktualizujcie system operacyjny, aplikacje i oprogramowanie – w tym antywirusy. Stosujcie silne, bezpieczne hasła, a najlepiej uwierzytelnianie dwuskładnikowe. Twórzcie też kopie zapasowe (backup), co pomoże Wam odzyskać dane bez potrzeby „negocjacji” z przestępcami.

ROOTKIT - daje cyberprzestępcom dostęp do Waszego urządzenia – zarówno do programów, jak i poszczególnych elementów systemu. Jest trudny do zlokalizowania, ponieważ potrafi wyłączać działające zabezpieczenia, niełatwo też jest się go pozbyć. Jeśli już uda się Wam go namierzyć, czasem jedyną deską ratunku jest ponowna instalacja systemu operacyjnego. Rootkit ma niejedno oblicze. Może zawierać w sobie wiele niebezpiecznych programów typu keylogger, spyware czy moduły przechwytujące hasła. Może też zagnieżdżać się w różnych miejscach systemu czy oprogramowania i niepostrzeżenie wyrządzać szkody. Nie zapominajcie o aktualizacjach , a przede wszystkim o zasadzie ograniczonego zaufania – z dużą ostrożnością podchodźcie do podejrzanych linków, nietypowych wiadomości, aplikacji i programów pochodzących z nieoficjalnych źródeł!

SCAM - Najczęstszą formą scamu jest masowa korespondencja elektroniczna (spam), jednak cyberprzestępcy grają na naszych emocjach również podczas kontaktów telefonicznych (spoofing, vishing). Ofiara jest przekonana, że odbiera telefon od policjanta, urzędnika czy też pracownika banku, dlatego bez oporów wykonuje wszelkie polecenia, np. podaje swoje dane osobowe lub dane do logowania. Scamerzy korzystają też z formularzy i fałszywych stron internetowych do złudzenia przypominających prawdziwe witryny banku czy urzędu. Bywa, że wysyłają e-maile, w których nakłaniają do kliknięcia linków prowadzących do takich stron. Oferty produktów w niskich cenach, nagrody bez udziału w konkursach, obietnica spadku po dalekim krewnym – to tylko niektóre przykłady scamu.

SKIMMING - Jest to oszustwo polegające na kopiowaniu przez złodzieja zawartości paska magnetycznego lub chipa z karty płatniczej, prowadzące do obciążenia rachunku bankowego okradanej osoby. Sprawcy przy pomocy tzw. skimmera – specjalnego urządzenia kopiującego umieszczanego w bankomacie – przechwytują informacje zawarte na karcie. Towarzysząca urządzeniu kopiującemu mikrokamera lub

„ABC CYBERBEZPIECZEŃSTWA”
ulotka promocyjna dla dzieci, młodzieży i rodziców w ramach Dnia Bezpiecznego Internetu 2024 w Zespole Szkolno-Przedszkolnym w Łysej Górze

specjalna nakładka na klawiaturę pozwalają ponadto rejestrować wpisywany przez użytkownika PIN.
Jak się ustrzec przed utratą gotówki? Korzystajcie z bankomatów położonych w uczęszczanych i dobrze oświetlonych miejscach, rezygnujcie z wypłat, gdy cokolwiek wzbudzi Wasze podejrzenia. Jak oka w głowie strzeżcie też swojej karty i numeru PIN – nie przekazujcie karty innym osobom i nie zapisujcie numeru PIN na karteczce noszonej w portfelu ani na samej karcie płatniczej.

SMISHING - drogą ataku są wiadomości tekstowe lub SMS. Wiadomość z żądaniem niewielkiej dopłaty do przesyłki od firmy kurierskiej czy do ostatniego rachunku za prąd od dostawcy energii, SMS z banku o blokadzie naszego konta wraz z linkiem do jego odblokowania albo przypomnienie o rozliczeniu podatku. Oszuści wysyłają wiadomości na przypadkowe numery (mają do dyspozycji dużą, ale przecież ograniczoną pulę dziewięciocyfrowych numerów) – wiedzą, że część z nich trafi do realnych odbiorców, którzy odpowiedzą na SMS. Nie klikajcie w linki takich wiadomości.

SPOOFING - To rodzaj popularnego oszustwa polegający na podszywaniu się pod konkretną osobę lub podmiot (np. instytucję, firmę) w celu pozyskania istotnych informacji lub wyłudzenia pieniędzy. Przestępcy przejmują wybrany numer telefonu i dzwonią do ofiary, podając się np. za pracownika banku, przedstawiciela znanej instytucji czy osobę publiczną. Żądają przykładowo zainstalowania wskazanej aplikacji, która ma nas rzekomo uchronić przed utratą pieniędzy. Waszą czujność powinna wzbudzić każda podejrzana wiadomość, w której nadawca – na pierwszy rzut oka wiarygodny – prosi o podanie poufnych danych czy loginów i haseł do bankowości internetowej.
Jak chronić się przed spoofingiem? Włączcie zasadę ograniczonego zaufania. Nie odpowiadajcie na żadne próby wyłudzenia poufnych informacji, sprawdzajcie dokładnie, czy na pewno logujecie się w oknie prawdziwej strony, omijajcie szerokim łukiem te platformy, które po prostu wydają się Wam dziwne. Podejrzane witryny zgłaszajcie do CERT Polska za pośrednictwem formularza na stronie incydent.cert.pl. A jeśli macie podejrzenie, że doszło do kontaktu telefonicznego z potencjalnym oszustem, rozłączcie się i sprawdźcie (np. dzwoniąc do banku), czy taka rozmowa w ogóle powinna mieć miejsce.

SPYWARE - Oprogramowanie to zaraża komputer, telefon lub inne urządzenie, aby gromadzić nasze dane oraz ważne informacje, np. o sposobach korzystania z internetu. Złośliwe działania tych programów obejmują przechwytywanie naciśnięć klawiszy (keylogger), zrzutów ekranu, poświadczeń uwierzytelniających, danych z formularzy internetowych i innych danych osobowych, w tym numerów kart kredytowych. Oprogramowanie szpiegujące rozprzestrzenia się w formie trojanów, wirusów i innych złośliwych programów. Uważajmy też na pozornie przydatne narzędzia czy aplikacje, darmowe oprogramowanie, a nade wszystko – linki i załączniki w podejrzanych e-mailach. Aby chronić się przed oprogramowaniem szpiegującym, nadrzędne jest zachowanie zasady ograniczonego zaufania – nie otwierajcie wiadomości od nieznanych nadawców, nie klikajcie w podejrzane linki i nie pobierajcie załączników (chyba że pochodzą z pewnego źródła). Zawczasu zaopatrzcie się też w program antywirusowy, który zapewnia ochronę w czasie rzeczywistym i zablokuje potencjalnego szpiega, zanim ten zdąży uruchomić się na komputerze.

STEALWARE - oprogramowanie szpiegujące które zbiera informacje o użytkowniku, by następnie przekazać pozyskane dane osobom trzecim. Przedostaje się do systemu za pomocą odpowiednio przegotowanych robaków i wirusów oraz dzięki wykorzystaniu luk czy błędów w przeglądarkach internetowych. Stealware potrafi np. śledzić aktywność użytkownika na platformach z płatnością elektroniczną, by w odpowiednim momencie podmienić numer konta, przez co jego środki trafią do zupełnie innego odbiorcy niż zamierzał.
Jak chronić się przed stealware? Przede wszystkim unikajcie pobierania „przydatnych”, darmowych narzędzi z nieznanych źródeł. Ponadto dbajcie o swoje urządzenia – aktualizujcie system, programy, antywirusy. Nie klikajcie w podejrzane linki i reklamy.

TABNABBING - polegający na podmianie zawartości strony internetowej. Jego celem jest wyłudzenie danych, do którego dochodzi po zalogowaniu się na fałszywej stronie, spreparowanej przez cyberprzestepcę. Tabnabbing wykorzystuje nawyk korzystania z wielu kart w przeglądarce. Podmienia zawartość nieużywanej strony na swoją – fałszywą (która udaje np. popularny serwis społecznościowy, pocztę e-mail, a nawet stronę bankowości internetowej) i próbuje wyłudzić od Was dane logowania – np. zmuszając do ponownego zalogowania się do konta, z którego pozornie zostaliście wylogowani. Nie pozostawiajcie przez długi czas otwartych kart ze stronami, które wcześniej przeglądaliście.

VISHING - odnosi się do wyłudzania poufnych danych lub pieniędzy podczas rozmowy telefonicznej. Cyberprzestępcy dzwonią do ofiar, podszywają się np. pod pracownika banku, urząd skarbowy bądź inną znaną instytucję i próbują zmanipulować ofiarę, wyłudzić od niej informacje, pieniądze, a nawet dostęp do komputera – instalując na nim oprogramowanie pozwalające na zdalną kontrolę nad urządzeniem. Cyberprzestępcy wykorzystują w tym ataku także spoofing, w którym przejmują wybrany numer telefonu i dzwonią do ofiary, podając się np. za przedstawiciela znanej instytucji, banku, a nawet osobę publiczną. Najważniejsza jest więc ostrożność, spora dawka podejrzliwości oraz niepodejmowanie pochopnych działań – tym bardziej, gdy rozmówca naciska na Was, straszy lub oczekuje bardzo szybkiej reakcji. W takiej sytuacji najlepiej samodzielnie skontaktować się z instytucją – np. wybierając się do oddziału lub dzwoniąc na infolinię podaną na oficjalnej stronie. Pamiętajcie jednak, by nie oddzwaniać na numer zapisany w rejestrze połączeń w telefonie, nawet jeśli wydaje się Wam prawdziwy, ponieważ może on należeć do przestępcy.

„ABC CYBERBEZPIECZEŃSTWA”
ulotka promocyjna dla dzieci, młodzieży i rodziców w ramach Dnia Bezpiecznego Internetu 2024 w Zespole Szkolno-Przedszkolnym w Łysej Górze

TO WARTO WIEDZIEĆ

CERT Polska (Computer Emergency Response Team Polska) – czyli zespół reagowania na incydenty działający w strukturach NASK – Państwowego Instytutu Badawczego. Do zadań CERT Polska należą: monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym, reagowanie na otrzymane zgłoszenia, wydawanie komunikatów o zidentyfikowanych niebezpieczeństwach, współpraca z podobnymi jednostkami na całym świecie czy prowadzenie działań z zakresu budowania świadomości w obszarze cyberbezpieczeństwa.

Dyżurnet.pl To zespół ekspertów NASK działający jako punkt kontaktowy do zgłaszania nielegalnych treści w internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci. Dyżurnet.pl m.in. obsługuje linię telefoniczną i serwis internetowy, umożliwiając zgłaszanie i analizę przypadków dystrybucji, rozpowszechniania lub przesyłania materiałów przedstawiających seksualne wykorzystywanie dzieci, w skrócie CSAM (z ang. child sexual abuse materials), przez internet. Zgłoszenia o potencjalnie nielegalnych treściach możecie przekazywać za pomocą formularza, na adres mailowy dyzurnet@dyzurnet.pl lub pod numerem telefonu 801 615 005.

Helpline To inaczej linia pomocowa, czyli numer telefonu, pod którym możecie uzyskać poradę specjalisty, emocjonalne wsparcie w trudnej sytuacji lub po prostu zostać wysłuchanym. Pamiętajcie, że na zdrowie psychiczne dorosłych, ale też dzieci i młodzieży, ma wpływ wiele czynników, w tym problemowe użytkowanie sieci i urządzeń cyfrowych. Do internetu przenoszą się bowiem tradycyjne problemy, takie jak hejt, agresja, przemoc rówieśnicza, wykluczanie z grona „znajomych”. Nie należy lekceważyć żadnych przejawów cyberprzemocy, a jeśli wymaga tego sytuacja – kontaktować się ze specjalistami. Podpowiadamy, gdzie możecie uzyskać rzetelną pomoc, gdy tylko poczujecie, że znaleźliście się w sytuacji bez wyjścia.

• 116 111 (116111.pl) – Bezpłatny i anonimowy telefon zaufania dla dzieci
• 116 123 – Bezpłatny kryzysowy telefon zaufania dla dorosłych
• 800 100 100 (800100100.pl) – Bezpłatny i anonimowy telefon zaufania dla rodziców i nauczycieli
• 800 70 2222 (liniawsparcia.pl) – Centrum wsparcia dla osób w stanie kryzysu psychicznego • 800 12 12 12 (brpd.gov.pl, e-mail: rpd@brpd.gov.pl) – Telefon zaufania Rzecznika Praw Dziecka

INCYDENT BEZPIECZEŃSTWA-To sytuacja, w której korzystając z internetu, możecie być narażeni na niebezpieczeństwo. W sieci codziennie możemy stać się ofiarą różnych prób cyberataków, dlatego warto na bieżąco śledzić informacje na temat metod stosowanych przez oszustów (a tych ciągle przybywa!) oraz pamiętać o zgłaszaniu incydentów bezpieczeństwa. Jak to zrobić? Z pomocą przychodzi CERT Polska, czyli zespół reagowania na incydenty. Aby zgłosić niebezpieczne zdarzenie, wypełnijcie formularz dostępny na stronie cert.pl, wyślijcie e-mail na adres: cert@cert.pl albo – w przypadku potencjalnie niebezpiecznej wiadomości SMS – przekażcie ją pod numer 799 448 084. Zgłoszenia dotyczące nielegalnych treści w internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci, powinniście przesyłać do zespołu Dyżurnet.pl. W tym celu można skorzystać z formularza, wysłać wiadomość na e-mail (dyzurnet@dyzurnet.pl) lub zadzwonić na infolinię: 801 615 005. Pamiętajcie, że incydenty należy zgłaszać jak najszybciej – dzięki temu inni użytkownicy internetu będą mogli uchronić się przed zagrożeniami.

NASK Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB) działa od 1991 r., a naszą misją jest cyfryzacja kraju oraz zapewnienie bezpieczeństwa w cyberprzestrzeni. Instytut prowadzi działalność naukową i badawczą (ThinkStat) oraz realizuje projekty edukacyjne (Akademia NASK, Safer Internet, ESA – Edukacyjna Sieć Antysmogowa), przekazując dzieciom i młodzieży wiedzę na temat zagrożeń w internecie. Promuje też koncepcję społeczeństwa informacyjnego otwartego na nowe technologie. Ponadto, zgodnie z Ustawą o krajowym systemie cyberbezpieczeństwa, NASK pełni obowiązek jednego z Zespołów Reagowania na Incydenty Komputerowe – CSIRT (incydenty bezpieczeństwa i potencjalnie nielegalne treści można zgłaszać do CERT Polska i zespołu Dyżurnet.pl). W ramach partnerstwa z Kancelarią Prezesa Rady Ministrów realizujemy też strategiczne projekty, takie jak: Ogólnopolska Sieć Edukacyjna (OSE), EZD RP – System Elektronicznego Zarządzania Dokumentami. Prowadzimy również Rejestr Domeny .pl oraz nowatorskie projekty w obszarze biometrii, usług Big Data czy sztucznej inteligencji. Dowiedzcie się więcej o NASK-PIB – wejdźcie na stronę nask.pl.

Polskie Centrum Programu Safer Internet (PCPSI) W NASK aktywnie działamy na rzecz bezpieczeństwa dzieci i młodzieży korzystających z internetu i nowych technologii, m.in. jesteśmy koordynatorem projektu Polskie Centrum Programu Safer Internet. Na działania PCPSI składają się trzy projekty:

1. Saferinternet.pl: projekt, w którym zwiększamy społeczną świadomość na temat zagrożeń w cyberprzestrzeni. Publikacje powstające w ramach projektu oraz organizowane konferencje kształtują kompetencje – dzieci, rodziców i profesjonalistów – w zakresie bezpiecznego korzystania z sieci. Z naszymi działaniami docieramy zarówno do młodszych (np. Sieciaki, Necio, Plik i Folder, Digital Youth), jak i starszych użytkowników internetu (np. Dzień Bezpiecznego Internetu, Międzynarodowa Konferencja „Bezpieczeństwo dzieci i młodzieży w internecie”).
2. Pomoc telefoniczna i online: realizujemy ją poprzez Telefon zaufania dla dzieci i młodzieży (116 111) oraz Telefon dla rodziców i nauczycieli w sprawach bezpieczeństwa dzieci (800 100 100). Eksperci Fundacji Dajemy Dzieciom Siłę za ich pośrednictwem reagują w przypadkach zagrożeń związanych z korzystaniem z internetu.
3. Dyżurnet.pl: to punkt kontaktowy, który prowadzimy w NASK. Możecie do niego anonimowo zgłaszać przypadki występowania w internecie nielegalnych treści, w tym materiałów przedstawiających seksualne wykorzystanie dzieci (formularz zgłoszeniowy, tel.: 801 615 005, e-mail: dyzurnet@dyzurnet.pl).

„ABC CYBERBEZPIECZEŃSTWA”
ulotka promocyjna dla dzieci, młodzieży i rodziców w ramach Dnia Bezpiecznego Internetu 2024 w Zespole Szkolno-Przedszkolnym w Łysej Górze

Więcej informacji o działaniach w ramach PCPSI znajdziecie na stronie saferinternet.pl