Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM WYDANIU..

- Wstęp
- Podstawy
- Dzieci w odwiedzinach

Naucz swoje dzieci cyberbezpieczeństwa

Wstęp

Istnieje bardzo dużo sposobów, w które dzieci mogą uzyskać dostęp do sieci i komunikować się z innymi jej użytkownikami. Nowe media społecznościowe nieustannie pojawiają się i znikają, tak samo jak liczba aplikacji, które korzystają z sieci Internet. Wiele szkół zaczyna również korzystać z usług takich jak Dysk Google i wymagają, aby zadania domowe były przesyłane przez Internet. Dzieci dorastają będąc nieustannie podłączone do sieci. Oczywiście niesie to ze sobą wiele możliwości, ale i niebezpieczeństw. W tym wydaniu biuletynu zwrócimy uwagę na obszary związane z zagrożeniami i podamy sposoby, które pozwolą na ich uniknięcie.

Redaktor gościnny

Bob Rudis pracuje w firmie Verizon jako pracownik naukowy w zakresie analizy danych. Jest też autorem raportu na temat wycieków danych (2015 Data Breach Investigations Report) jak i ojcem czwórki dzieci. Bob stworzył i prowadził szkolenia zwiększające świadomość zagrożeń w cyberprzestrzeni dla wielu firm z listy Fortune 100. Możesz znaleźć Boba na Twitterze: **@hrbrmstr**.

Zagrożenia

1. **Zachowania**: W świecie wirtualnym, dzieci mogą zachowywać się inaczej niż w życiu codziennym. Brak bezpośredniego kontaktu może spowodować, że dzieci zaczną się czuć anonimowo. Często również mogą angażować się w nieodpowiednie, raniące zachowania jak cyberprzemoc czy trollowanie. Twoje dzieci mogą także paść ofiarą osób, które chcą im umyślnie wyrządzić krzywdę.

2. **Kontakty**: Dzieci niemal nieustannie komunikują się z innymi, czy to poprzez wiadomości SMS, czy na forach i czatach internetowych czy nawet w wirtualnych światach. Brak fizycznego kontaktu może powodować, że dzieci staną się bardziej ufne i mogą wziąć osobę, z którą rozmawiają za kogos innego. Osoby uwodzące używają różnych narzędzi, aby zbudować relację z potencjalną ofiarą, często podszywając się pod rówieśników.

3. **Zawartość**: Istnieje bardzo wiele sposobów, które pozwalają umieścić obraz, dźwięk czy film w Internecie. Prawdopodobieństwo, że dzieci będą się dzielić większą liczbą informacji niż powinny jest bardzo realne. Powoduje to, że mogą stworzyć niebezpieczeństwo nie tylko dla dziecka, ale także dla Ciebie i Twojej rodziny. Dzieci mogą sobie także nie zdawać sprawy z zagrożenia jakie powoduje kradzież tożsamości czy kliknięcie w linki przysłane od nieznanych osób. Żyjemy w czasach, w których informacje znajdujące się w sieci nie mogą zostać usunięte. Dzieci mogą myśleć, że ich posty na Instgramie, Kik czy Snapchat znikną po wyświetleniu, ale mogą też zostać zapisane

Naucz swoje dzieci cyberbezpieczeństwa

przez innych użytkowników i wykorzystane później w celu prześladowania dzieci lub ich rodzin w najmniej oczekiwanym momencie.

Jak informować dzieci?

Najważniejsza jest rozmowa z dziećmi. Bądź świadom jak korzystają z sieci, uświadom je jakie zagrożenia na nie czyhają i co powinny zrobić, żeby się przed nimi obronić.

Aby ochronić dzieci w sieci Internet, poinformuj je o zagrożeniach i upewnij się, że dzieci rozmawiają z Tobą o tym, co je spotyka.

1. **Bezpieczeństwo w domu**: Dla dzieci to dom jest miejscem gdzie zaczyna się edukacja na temat bezpieczeństwa online. Im wcześniej zaczniesz rozmawiać ze swoimi dziećmi tym lepiej. Regularnie przeprowadzaj rozmowy ze swoimi najmłodszymi na temat bezpieczeństwa w sieci. Podaj przykłady złych zachowań. Jeśli nie wiesz co Twoje dzieci robią w Internecie to po prostu je o to zapytaj. Udawaj, że nie znasz się na najnowszych technologiach i poproś dziecko, aby Ci wytłumaczyło jak działają i jak ich używają. Dzieci uwielbiają odgrywać rolę nauczycieli i z chęcią Cię poinstruują. Na przykład, poproś, aby Ci pokazały jak działa Instagram, nauczyły Ciebie jego obsługi, założyły Ci konto, za pomocą którego możesz monitorować ich działania. Dzięki temu nie tylko nauczysz się czegoś nowego, ale ułatwisz im komunikację z Tobą. Ustal, że korzystanie z Internetu odbywa się tylko w często uczęszczanych miejscach domu czy mieszkania i wyznacz godziny korzystania z sieci. Przez to, że ktoś będzie często przechodził obok używanego komputera, dzieci mogą nie chcieć angażować się w niebezpieczne zachowania. Rozważ także stworzenie specjalnej centralnej stacji ładowania telefonów, gdzie wszystkie urządzenia są ładowane w nocy.

2. **Bezpieczeństwo poza domem**: podczas pobytu poza domem dzieci są bardziej narażone na ryzyko. Niech zrozumieją, że zasady nie istnieją tylko w domu, ale są niezależne od tego gdzie i z kim się komunikujesz. Powiedz o swoich zasadach także osobie, pod opieką której pozostawiasz dziecko. Jeśli Twoje dzieci używają telefonów komórkowych sprawdź, czy użycie danych mobilnych nie zwiększa się podczas ich nieobecności w domu. Nie będziesz w stanie powstrzymać wszelkich niebezpieczeństw, ale być może Twoje słowa pozostaną w pamięci dzieci, kiedy będą chciały skorzystać z internetu mobilnego.

3. **Bezpieczeństwo w grupie**: nie powinieneś sam próbować pilnować swojego dziecka. Do pomocy zaangażuj innych rodziców, opiekunów, rodzeństwo, nauczycieli i przyjaciół. Niech zwracają uwagę na niebezpiecznej zachowania Twojego dziecka. Zachęcaj swoich najbliższych i otoczenie, aby zwracali uwagę na to, co dzieci robią w Internecie i odpowiednio reagowali na zauważone problemy.

Naucz swoje dzieci cyberbezpieczeństwa

Jeśli jednak dziecko popełni błąd, wykorzystaj to jako okazję, żeby je czegoś nauczyć, a nie tylko ukarać. Za każdym razem wytłumacz dlaczego to co zrobiły jest złe i przypomnij, że starasz się je uchronić przed niebezpieczeństwami, których jeszcze nie rozumieją. Poinformuj je, że zawsze mogą do Ciebie przyjść, jeśli tylko poczują się niekomfortowo. Możesz poprosić nawet o wykonanie zrzutu ekranu takiej sytuacji, aby móc lepiej ocenić co się stało. Upewnij się, że czują się komfortowo w rozmowie z Tobą, nawet jeśli zrobiły coś nieodpowiedniego. Utrzymywanie otwartej i stałej komunikacji ze swoim dzieckiem jest najlepszym zabezpieczeniem przed cyberzagrożeniami.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego.
Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Przydatne linki

Strona polskiego centrum programu SaferInternet: http://www.securingthehuman.org/ouch/2014#november2014

Strona zespołu zajmującego się nieodpowiednimi treściami w Internecie: https://dyzurnet.pl/

Materiały multimedialne dla dzieci prezentujące zagrożenia: http://saferinternet.pl/pl/multimedia-cyberprzemoc

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski