Biuletyn Bezpieczeństwa Komputerowego

Bezpieczeństwo dzieci online

Informacje ogólne

Dzieci korzystają z internetu więcej niż kiedykolwiek, używają go żeby kontaktować się z przyjaciółmi i rodziną, do nauki i rozrywki. Jak więc możemy pomóc naszym dzieciom w bezpiecznym korzystaniu z technologii online?

Edukacja i komunikacja

Po pierwsze, upewnij się że masz dobrą komunikację ze swoimi dziećmi. Często zdarza się, że rodzice zostają zaangażowani w blokowanie treści lub decydowanie, które aplikacje są dobre, a które złe. Zazwyczaj bezpieczeństwo dzieci w mniejszym stopniu zależy od technologii, a bardziej od zachowania i wpojonych wartości. Na początek warto stworzyć listę oczekiwań od dzieci. Oto kilka rzeczy do rozważenia (te zasady powinny ewoluować wraz z wiekiem dzieci):

- Ustal czas, w którym mogą lub nie mogą korzystać z Internetu i jak długo mogą to robić. Upewnij się że dzieci wykonały wszystkie prace domowe lub obowiązki zanim zaczną grać online lub korzystać z sieci społecznościowych ze znajomymi, a także ogranicz im ilość czasu spędzanego online każdego dnia.
- Określ rodzaje stron internetowych oraz gier, z których mogą korzystać i dlaczego są one odpowiednie lub nie.
- Ustal jakie informacje mogą udostępniać i komu. Dzieci często nie zdają sobie sprawy, że to co publikują nie znika i staje się publiczne. W dodatku to co udostępnią prywatnie swoim znajomym, może być (i często jest) udostępnione innym bez ich wiedzy.
- Poinformuj komu powinny zgłaszać problemy, takie jak dziwne wyskakujące okienka, podejrzane witryny internetowe lub nieodpowiednie zachowanie innych użytkowników Internetu. Bardzo ważne jest, aby dzieci czuły się bezpiecznie rozmawiając z zaufaną osobą dorosłą.
- Podobnie jak w prawdziwym świecie, naucz dzieci traktować innych w internecie tak, jak same chciałyby być traktowane.
- Upewnij się, że dzieci rozumieją, że osoby mogą nie być w rzeczywistości tymi, za kogo się podają i nie wszystkie informacje są prawdziwe.
- Zdefiniuj, co można kupić online i przez kogo, wliczając w to zakupy w grach.

Z biegiem czasu, im lepiej się dzieci zachowują i im więcej zaufania zdobywają, tym większą elastyczność można im zapewnić. Gdy zdecydujesz się na te zasady, niech będą one ogólnodostępne w domu. Jeszcze lepszym rozwiązaniem może być podpisanie "umowy". W ten sposób wszyscy będą w pełni zgodni.

Im wcześniej zaczniesz rozmawiać z dziećmi o swoich oczekiwaniach, tym lepiej. Jak zacząć rozmowę? Zapytaj dziecko z jakich aplikacji korzysta i jak one działają. Postaw swoje dziecko w roli nauczyciela i poproś, aby pokazało co robi online. Poproś o podanie kilku scenariuszy "Co by było, gdyby...", aby sprawdzić reakcję na rzeczy, które omówiliście lub uzgodniliście. Utrzymywanie otwartej i aktywnej komunikacji to najlepszy sposób na zapewnienie dzieciom bezpieczeństwa w dzisiejszym cyfrowym świecie.

W przypadku urządzeń mobilnych rozważ stworzenie w domu miejsca centralnej stacji ładującej. Zanim dzieci pójdą spać, ustal czas, w którym urządzenia mobilne należy umieścić w stacji ładującej, tak aby dzieci nie ulegały pokusie korzystania z nich, gdy powinny spać.

Technologie bezpieczeństwa i kontrola rodzicielska

Istnieją programy do kontroli rodzicielskiej, których można użyć do monitorowania i zapewnienia ochrony dzieciom. Te rozwiązania najlepiej sprawdzają się w przypadku młodszych dzieci. Starsze dzieci nie tylko potrzebują większego dostępu do internetu, ale często używają urządzeń, których nie kontrolujesz lub których nie możesz monitorować, takich jak te wydane przez szkołę, konsole do gier lub urządzenia w domach znajomych. Ponadto starsze dzieci są na tyle świadome, że potrafią obejść technologiczne próby kontroli. Dlatego tak ważne jest informowanie dzieci o swoich oczekiwaniach, ale jednocześnie warto mieć do nich zaufanie.

Dawanie przykładu

Dawaj dobry przykład jako rodzic lub opiekun. Kiedy rozmawiasz z dziećmi, odłóż telefon i porozmawiaj z nimi twarzą w twarz. Nie używaj urządzeń mobilnych przy stole i podczas jazdy samochodem. Kiedy dzieci popełniają błędy, traktuj każdy z nich jako doświadczenie, z którego można się uczyć, zamiast je karać. Upewnij się, że czują się bezpiecznie zwracając się do Ciebie, w momencie kiedy popełnili jakiś błąd.

Redaktor gościnny

Diana Kelley jest członkiem zarządu WiCyS i CISO w Protect AI. Jest instruktorką kursu LinkedIn Learning: Security Risks in AI (Artificial Intelligence) and ML (Machine Learning) oraz jest współautorką książki Practical Cybersecurity Architecture.

Źródła

Bezpieczne gry online: https://www.sans.org/newsletters/ouch/securely-gaming-online/
Prywatność - chroń swoje cyfrowe życie: https://www.sans.org/newsletters/ouch/privacy/
Bezpieczeństwo urządzeń mobilnych: https://www.sans.org/newsletters/ouch/securing-mobile-devices/
Naucz się nowej umiejętności - wykrywanie Deepfake: https://www.sans.org/newsletters/ouch/learn-a-new-survival-skill-spotting-deepfakes/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz