# Bezpieczeństwo w sieci dla całej rodziny

Obecny czas, to przede wszystkim wytężona praca zdalna Uczniów, Rodziców i Nauczycieli. Wszyscy korzystamy z internetu, dlatego warto przekazać dzieciom umiejętności, dzięki którym będą mogły poruszać się w sieci w przyjemny i bezpieczny sposób.

Znajdziecie tu Państwo zestaw zagadnień związanych z obecnością dzieci w internecie. A na ostatnich stronach zamieszczony jest słowniczek kluczowych pojęć związanych z cyberbezpieczeństwem. ☺

## KODEKS BEZPIECZEŃSTWA

**ROZSĄDEK** — Udostępniaj z głową, czyli co można, a czego lepiej nie udostępniać w internecie.

**UWAŻNOŚĆ** — Nie daj się nabrać, czyli jak dostrzec, czy coś jest prawdziwe czy nie, co jest kłamstwem, a co oszustwem internetowym.

**SIŁA** — Chroń swoje sekrety, czyli jak tworzyć silne hasła oraz zapewnić bezpieczeństwo.

**ŻYCZLIWOŚĆ** — Życzliwość jest fajna, czyli co to znaczy być uprzejmym online i szanować prywatność innych osób.

**ODWAGA** — Rozmawiaj o wątpliwościach, czyli jak w trudnych sytuacjach poprosić o pomoc rodzica lub inną zaufaną osobę dorosłą.

# Udostępniaj z głową

Dzieci, podobnie jak niektórzy dorośli, uwielbiają dzielić się online. Udostępniają wszystko, od zdjęć swojego kota po zabawne filmiki, które chcą pokazać wszystkim znajomym. Problem polega jednak na tym, że młodsze dzieci czasami nie rozumieją, że to, co dziś publikują w internecie, ktoś będzie mógł zobaczyć w odległej przyszłości, lub że niektóre rzeczy najlepiej zachować w tajemnicy.

Drogi Rodzicu:

- Przypomnij dziecku, aby przyszło do ciebie lub innej zaufanej osoby dorosłej, jeśli coś poszło nie tak, abyś mógł/mogła szybko zadziałać. Możesz pomóc mu zablokować, usunąć i zgłosić innych użytkowników.
- Porozmawiaj ze swoim dzieckiem o rzeczach, którymi bez wątpliwości można się dzielić online, np. zabawnym, nieobraźliwym filmikiem z kotem wysłanym do przyjaciół. Zachęcanie do właściwego zachowania w internecie jest naprawdę ważne. Pozytywne wykorzystanie technologii to jedna z rzeczy, które gwarantują bezpieczeństwo dzieci w internecie.

# Nie daj się nabrać

Nie wszystko, na co twoje dziecko natknie się w internecie, jest prawdziwe lub wiarygodne. Największa trudność polega na dostrzeganiu różnic. Uczenie się, jak rozpoznać wskazówki dotyczące tego, co jest prawdziwe, a co fałszywe, co jest kłamstwem lub oszustwem internetowym, pomoże dziecku pewnie poruszać się online i uważać na to, co zobaczy i przeczyta.

Drogi Rodzicu:

- Usiądź razem z dzieckiem, weźcie tablet lub inne urządzenie i przejdźcie do swojej ulubionej wyszukiwarki, wpiszcie tematykę, którą interesuje się dziecko i przejrzyjcie razem wyniki wyszukiwania. Obejrzyjcie je i zadajcie sobie wspólnie kilka pytań:
    - ❖ Czy widać, kto jest autorem strony? Jeśli tak, czy jest to ktoś znany?
    - ❖ Czy język na stronie jest wyraźnie emocjonalny?
    - ❖ Czy jest to strona sponsora albo fana (więc może jest głównie pozytywna)?
    - ❖ Jeśli informacje są negatywne, czy możesz dowiedzieć się więcej o samej witrynie i źródle krytyki?

- ❖ Czy to subiektywna opinia / blog tylko jednej osoby czy raczej wydaje się neutralna?
- ❖ Jeśli to witryna z wiadomościami (serwis informacyjny), to czy jest ci dobrze znana i możesz jej zaufać, czy raczej chcesz dowiedzieć się więcej na jej temat albo sprawdzić, czy inni czytelnicy sądzą, że próbuje przedstawić informacje w bezstronny sposób?
- ❖ Czy adres WWW strony jest prawidłowy (np. czy nie zawiera literówki lub jest w innej domenie krajowej niż ta, którą znasz)?
- ❖ Jeśli jest to strona służąca do logowania, czy ma adres zaczynający się od https://?

- Zachęcaj dziecko, żeby mówiło ci o stronach, które według niego/niej są godne zaufania, czyli wiarygodne i bezpieczne. Czy potrafi wymienić cechy godnej zaufania (czyli wiarygodnej i bezpiecznej) strony internetowej?
- Porozmawiaj z dzieckiem o uprzedzeniach – ustal, czy potrafi określić pobudki, jakimi kieruje się autor. Sprawdź, czy potrafi dostrzec błędy ortograficzne i gramatyczne, które mogą świadczyć o nierzetelności strony internetowej.
- Porozmawiaj z dzieckiem o elementach, które świadczą o tym, że strona jest bezpieczna od strony technicznej. Ustal, czy wie, kiedy może podać swoje dane podczas logowania.

## Chroń swoje sekrety

Wiemy, że niektóre informacje muszą pozostać prywatne. Dla młodszych dzieci to może być trudne do zrozumienia. Może im się wydawać, że dzielenie się hasłami z najlepszymi przyjaciółmi jest w porządku. Prawdopodobnie nie będą wiedzieć, że w internecie niektórzy ludzie działają na szkodę innych i próbują wykraść ich informacje.

Drogi Rodzicu:

- Zacznij od swobodnej rozmowy. Zapytaj swoje dziecko, czy uważa, że hasło „123” jest mocne (bezpieczne). Porozmawiajcie o tym, dlaczego ważne jest posiadanie takiego hasła, które tobie jest łatwo zapamiętać, ale nikt inny go nie zgadnie.
- Napiszcie razem przepis na silne hasło i zawrzyjcie w nim wszystkie składniki potrzebne do stworzenia bezpiecznego hasła do kont online i konkretne instrukcje, jak je ułożyć.
    - ❖ Przykładowe składniki:

- 3 wielkie litery
- 4 lub więcej małych liter
- 2 symbole
- 1 cyfra.

- Spróbujcie utworzyć inne hasło dla każdego konta online, aby nie używać wszędzie jednakowych.
- Nie udostępniajcie haseł nikomu (nawet najlepszemu przyjacielowi).
- Słabe hasło to takie, które łatwo odgadnąć, jak np. imię twojego zwierzaka.
- Pomieszajcie wielkie i małe litery.
- Unikajcie używania imion i nazwisk, imienia zwierząt domowych, daty urodzenia i innych oczywistych informacji, które mogą ułatwić innym odgadnięcie hasła.
- Dołączcie liczby i symbole, aby utrudnić odgadnięcie lub zhakowanie (złamanie) hasła.
- Używajcie krótkiego zdania zamiast jednego słowa, które dla innych będzie trudne do odgadnięcia, a dla ciebie łatwe do zapamiętania.

# Życzliwość jest fajna

Młodsze dzieci często nie zdają sobie sprawy, że niektóre wiadomości w sieci mogą zostać zrozumiane inaczej, niż chciał ich autor. Jeśli są świadkami nieuprzejmych zachowań, powinny zareagować. Czasami to, co nam wydaje się udostępnionym publicznie nieszkodliwym żartem, może zawstydzić i zdenerwować innych użytkowników internetu, a nawet naszych przyjaciół.

Drogi Rodzicu:

- To naturalne, że poszczególni członkowie rodziny mogą mieć odmienne zdanie na temat różnych sytuacji w internecie.
- Jeśli w internecie spotyka kogoś coś złego, nawet dziecko może aktywnie się przeciwstawić, zidentyfikować niepokojącą sytuację i zadziałać – najważniejsze, by nie pozostawać obojętnym. Odpowiedzialność społeczna naszych dzieci kształtuje się, gdy stają w obronie tego, co słuszne i próbują chronić innych, gdy dzieje się im krzywda.
- Nawet jeśli nie czujesz się ekspertem w dziedzinie technologii, możesz pomóc dzieciom rozwiązać ich problemy. Wytłumacz dziecku, że powinno przyjść do ciebie lub innej zaufanej osoby dorosłej, jeśli cokolwiek wzbudza jego niepokój.

- Wyjaśnij, że często błędnie rozumiemy wiadomości tekstowe, które nie są wypowiedziane głośno, twarzą w twarz. Możecie razem wymyślić jakieś przykłady. ☺

## SŁOWNICZEK ☺

# Udostępniaj z głową...

**Cyfrowy ślad**

Twój cyfrowy ślad to wszystko, co składa się na wizerunek twojej osoby w internecie. Tworzą go zdjęcia, nagrania audio, wideo, teksty, posty na blogach i wiadomości, które piszesz na stronach znajomych.

**Granice osobiste**

Zasady, które ustalasz, aby dać innym do zrozumienia, jak powinni się wobec ciebie zachowywać w bezpieczny i akceptowalny sposób.

**Informacje osobowe**

Informacje o konkretnej osobie. Informacje o tobie mogą być mniej lub bardziej publiczne/prywatne w zależności od stopnia ich wrażliwości.

**Ustawienia**

Obszar w dowolnej usłudze cyfrowej, aplikacji, witrynie internetowej itp., w którym można zdefiniować lub dostosować zakres udostępnianych im informacji i określić zasady obsługiwania konta.

# Nie daj się nabrać...

**Zaszyfrowany**

Informacje lub dane przekształcone w kod.

**Zapora / Firewall**

Program, który chroni komputer przed większością oszustw i włamań dokonywanych przez hakerów.

**Złośliwe oprogramowanie**

Termin odnoszący się do różnych form wrogiego lub niepożądanego oprogramowania, takiego jak wirusy komputerowe i inne szkodliwe programy.

**Phishing**

Atak phishingowy ma miejsce, gdy ktoś próbuje nakłonić użytkownika do udostępnienia danych osobowych online. Wyłudzanie informacji odbywa się zazwyczaj za pośrednictwem e-maila, reklam lub witryn, które wyglądają podobnie do stron, z jakich już korzystasz.

| | |
|---|---|
| **Scam** | Nieuczciwa próba zarobienia pieniędzy lub zdobycia czegoś wartościowego na drodze oszustwa. |
| **Phishing profilowany (spear phishing)** | Wyrafinowana forma oszustwa, w której cyberprzestępca wykorzystuje wszelkie dostępne w sieci informacje na temat ofiary, żeby obniżyć jej czujność i zainfekować komputer lub wykraść dane. |

## Chroń swoje sekrety...

| | |
|---|---|
| **Haker** | Osoba korzystająca z komputera w celu uzyskania dostępu do prywatnych informacji bez zezwolenia. |
| **Prywatność** | Ochrona informacji o tobie i innych osobach. |
| **Bezpieczeństwo** | Poleganie na dobrych nawykach w celu zabezpieczania sprzętu i oprogramowania. |
| **Scammer** | Ktoś, kto oszukuje lub podstępem przekonuje kogoś innego, by ujawnił swoje prywatne informacje albo nawet oddał pieniądze. |
| **Weryfikacja dwuetapowa** | Forma zabezpieczenia, w której logowanie do usługi wymaga dwóch kroków. Na przykład może być konieczne wprowadzenie hasła i kodu wysłanego w wiadomości SMS. |

## Życzliwość jest fajna...

| | |
|---|---|
| **Blokowanie (kogoś)** | Sposób na ograniczenie komuś dostępu do twojego profilu, możliwości wysyłania wiadomości itp. |
| **Bierny obserwator** | Ktoś, kto ma prawo interweniować lub zgłaszać złe zachowanie, ale nie robi nic, by je powstrzymać. |
| **Dokuczanie** | Powodowanie nieprzyjemnych lub wrogich sytuacji w rozmowie lub działaniu, aby celowo sprawić komuś przykrość. |
| **Aktywny obserwator** | Ktoś, kto interweniuje, aby powstrzymać i/lub zgłosić nieodpowiednie zachowanie. |

Opracowanie na podstawie projektu Asy Internetu – Fundacja Szkoła z Klasą
https://beinternetawesome.withgoogle.com/pl_all/