

## ***Załącznik nr 7***

### **Zasady dostępu małoletnich do internetu oraz ochrony przed szkodliwymi treściami**

Placówka, zapewniając małoletnim dostęp do internetu, jest zobowiązana podejmować działania zabezpieczające małoletnich przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju oraz bezpieczeństwa.

Zasady bezpiecznego korzystania z internetu i mediów elektronicznych uwzględnione zostały w regulaminie obowiązującym w pracowniach informatycznych.

#### **Zasady bezpiecznego korzystania z internetu**

### **1. Ogranicz dane osobowe, które udostępniasz w sieci**

Im mniej Twoich **danych osobowych** w sieci, tym lepiej – taka jest podstawowa zasada bezpiecznego korzystania z Internetu. Każda, nawet banalna informacja, może posłużyć przestępcom do ataku.

Imię i nazwisko, data urodzenia, numer karty kredytowej, numer PESEL, adres zamieszkania, bank, z którego usług korzystasz – to wszystko **informacje bezcenne dla cyberprzestępców**. Mogą wykorzystać je np. do phishingu (więcej na ten temat dowiesz się niżej) czyli **najbardziej popularnego rodzaju ataku** wymierzonego w każdego użytkownika sieci.

Im mniej prywatnych informacji podasz w Internecie, tym mniejsze ryzyko, że padniesz ofiarą np. **cyberstalkingu** czyli nękanie, groźb i ataków przy użyciu sieci.

### **2. Używaj silnych i unikalnych haseł**

Używanie **słabego hasła** lub jednego hasła do zabezpieczenia wielu kont, to recepta na kłopoty. Przestępca może okraść Twoje konto, zaciągnąć kredyt, użyć skrzynki e-mail do ataku na innych użytkowników czy też wykraść dane.

**Używaj silnych, nie powtarzających się haseł.** To podstawowa zasada higieny korzystania z m.in. bankowości elektronicznej, poczty e-mail i niezliczonej ilości usług w sieci, w których musisz używać hasła.

Hasła możesz tworzyć polegając na własnej przemyślności i sprawdzonych [porad dot. tworzenia silnych i trudnych do złamania haseł](#) lub skorzystać z [menedżera haseł](#). Menedżer haseł to program, który generuje i przechowuje dane logowania powiązane z kontami internetowymi. Dzięki niemu musisz pamiętać wszystkich haseł, wystarczy **hasło główne do menedżera**. Użycie takiego programu to praktyczny i zaawansowany sposób na poprawę bezpieczeństwa w sieci. Warto wybrać program typu open source z **szyfrowaniem typu end-to-end** i weryfikacją dwuskładnikową.

### **3. Używaj weryfikacji dwuetapowej**

**Weryfikacja dwuetapowa (2FA)** to opcja dostępna w wielu serwisach (Facebook, Google), która zdecydowanie poprawi Twoje cyberbezpieczeństwo. Tego typu uwierzytelnienie wymaga przynajmniej dwóch kroków: podania hasła oraz wprowadzenia tymczasowego kodu wysłanego przez serwis w sms-ie lub przy użyciu specjalnej aplikacji (np. Google Authenticator).

Możesz również zdecydować się na **stosowanie klucza U2F** czyli fizycznego przedmiotu przypominającego pendrive'a lub brelok do kluczy – ta metoda jest najbardziej odporna na phishing.

Pamiętaj, że uwierzytelnienie przy użyciu SMS jest mniej bezpieczne od dobrej aplikacji do weryfikacji dwuetapowej.

Oto **zestawienie weryfikacji 2FA** od najbardziej do najmniej bezpiecznych:

- klucz U2F,
- kody czasowe w aplikacji,
- kody jednorazowe SMS,
- kody wysyłane przez e-mail.

Dzięki uwierzytelnieniu wieloskładnikowemu skomplikujesz życie cyberprzestępcom i lepiej zabezpieczysz się jeżeli dane Twoje konta wyciekną lub zostaną wykradzione.

#### 4. Nie korzystaj z jednej skrzynki pocztowej

Wiele osób używa jednego adresu e-mail do obsługi spraw związanych z pracą/firmą, rejestracji do najróżniejszych newsletterów, zakupów czy też aplikacji w chmurze. To nie jest dobry pomysł.

Adres e-mail używany w celach służbowych/biznesowych często zawiera Twoje imię i nazwisko. Warto mieć **nieformalny adres mailowy**, który zapewni Ci większą [anonimowość w sieci](#). Ciekawym rozwiązaniem jest **Proton** – to cały ekosystem, którego celem jest zapewnienie użytkownikowi bezpieczeństwa podczas korzystania z sieci (dostępny również w opcji darmowej). Najbardziej ceniony jest [Proton Mail](#). To usługa, w której **każdy mail i załącznik jest zaszyfrowany** – odczyta go tylko zamierzony odbiorca. Proton korzysta z szyfrowania typu end-to-end (E2EE). E2EE uchodzi za **złoty standard zabezpieczenia komunikacji** w poczcie elektronicznej.

#### 5. Skasuj niepotrzebne/nieużywane konta

Im więcej masz kont założonych na różnych serwisach, tym **większe ryzyko wycieku** Twoich danych. Większość z nas ma konta na stronach, z których już nie korzysta. Dobrym pomysłem jest ich skasowanie.

#### 6. Uważaj na phishing i ransomware – podejrzane maile i SMS-y

Największym zagrożeniem w sieci jest [malware](#) czyli **złośliwe oprogramowanie**. Wśród takich programów prym wiodą ransomware i programy do phishingu.

## 7. Zainstaluj mocny program antywirusowy

Są osoby, które nie używają antywirusów. Jednak dla większości osób, to nie jest optymalne rozwiązanie. Antywirus da Ci spokojną głowę oraz **zabezpieczenie przed najbardziej popularnymi zagrożeniami**.

Dobrym pomysłem jest **przejrzenie testów programów antywirusowych** wykonanych przez niezależne laboratoria, m.in. AV-Comparatives i AV Test. Eksperti oceniają m.in. skuteczność ochrony, jak bardzo antywirus obciąża procesor komputera, jak często myli się ogłaszając fałszywe alarmy czy też jego zdolność obrony urządzenia przed zaawansowanymi atakami.

Inne kryteria wyboru to cena, dostępność na różne urządzenia i systemy operacyjne oraz **dotatkowe funkcje** oferowane przez producenta. Te dodatkowe funkcje to m.in. VPN, ochrona rodzicielska, menedżer haseł, szyfrowanie plików.

## 8. Używaj sieci Tor i/lub VPN

[Sieć Tor](#) to bardzo skuteczny sposób na bezpieczne i prywatne korzystanie z sieci. Zapytanie z komputera przechodzi przez kolejne węzły (serwery) i **jest szyfrowane**. Twój [adres IP](#) jest **maskowany**, a potencjalny obserwator nie wie jakie strony odwiedziłeś i co na nich robiłeś.

## 9. Unikaj przeglądania stron bez certyfikatu SSL

SSL to protokół sieciowy, który **służy do bezpiecznych połączeń** internetowych. Takie połączenia nawiązywane są przy użyciu certyfikatów – dlatego mówimy o [certyfikacie SSL](#). Strony z takim certyfikatem poznasz na pierwszy rzut oka – mają w adresie URL oznaczenie **https://** oraz symbol kłódki (w przeciwieństwie do stron **http://**).

**SSL szyfruje połączenie** między serwerem, a przeglądarką www. **Chroni dane**, które podajesz na odwiedzanych stronach – od imienia i nazwiska, przed adres e-mail, po numer karty kredytowej – przed dostępem niepowołanych osób. Takich informacji nie należy podawać na stronach z **http** czyli bez certyfikatu.

## 10. Zwiększ ustawienia prywatności na swoich kontach w mediach społecznościowych

Z zasady osoby, które korzystają z mediów społecznościowych mają **ograniczoną prywatność**. Właściciele serwisów zbierają informacje na temat ich zachowania w sieci, a potem wykorzystują do targetowania reklam lub **sprzedają zewnętrznym marketerom**.

Jeżeli chcesz być bardziej bezpieczny – mniej narażony na szpiegowanie i precyzyjnie dobierane reklamy – możesz **ograniczyć zakres informacji** zbieranych o tobie przez Facebooka, Twittera, Tik Toka czy Instagram. Zrobisz to w ustawieniach prywatności.

Dobrym pomysłem jest również ograniczenie innym osobom możliwości **oznaczania Cię na zdjęciach lub w wydarzeniach**. Po wprowadzeniu zmian zatwierdzisz lub odrzucisz tagowanie. Sprawdź również, kto może widzieć Twoje posty i mieć dostęp do informacji o wspólnych znajomych.

Serwisy społecznościowe często zmieniają regulaminy i wprowadzają nowe zasady dotyczące prywatności użytkowników. Regularnie monitoruj, co zbierają o tobie serwisy społecznościowe i reaguj w razie konieczności.

### **11. Aktualizuj system operacyjny i programy**

Jednym z poważniejszych zagrożeń w sieci są **złośliwe programy typu exploit**. To malware, które wyszukują luki w programach, a potem wykorzystują je do zainfekowania urządzenia innymi złośliwymi programami.

### **12. Zaszzyfruj dysk komputera i laptopa, zabezpiecz router i sieć WiFi**

Odpowiednie **zabezpieczenie urządzeń**, których używasz podczas korzystania z sieci, może przesądzić o bezpieczeństwie Twoich pieniędzy i danych.

Router to brama, która oddziela Twoją domową sieć od Internetu i czyhających w nim zagrożeń. Może być otwarta dla przestępców lub zamknięta i zabezpieczona solidnym zamkiem.

### **13. Zdobywaj wiedzę na temat bezpieczeństwa w sieci**

Wiedza to potężna broń – to zasada dotyczy również bezpiecznego korzystania z Internetu. Dodam: aktualizowana wiedza.

**Cyfrowy świat zmienia się każdego dnia.** Informacje sprzed roku o cyberzagrożeniach i sposobach ich zwalczania mogą być dzisiaj nieskuteczne. Warto sprawdzać dobre serwisy, które na bieżąco informują o najważniejszych wydarzeniach ze świata cyberbezpieczeństwa.

Rozmawiaj z dorosłymi o internecie, powiedz dorosłemu, któremu ufasz, gdy coś w internecie cię zaniepokoi.

**Za kontrolę tabletów, smartfonów używanych przez uczniów odpowiedzialni są rodzice/prawni opiekunowie!**