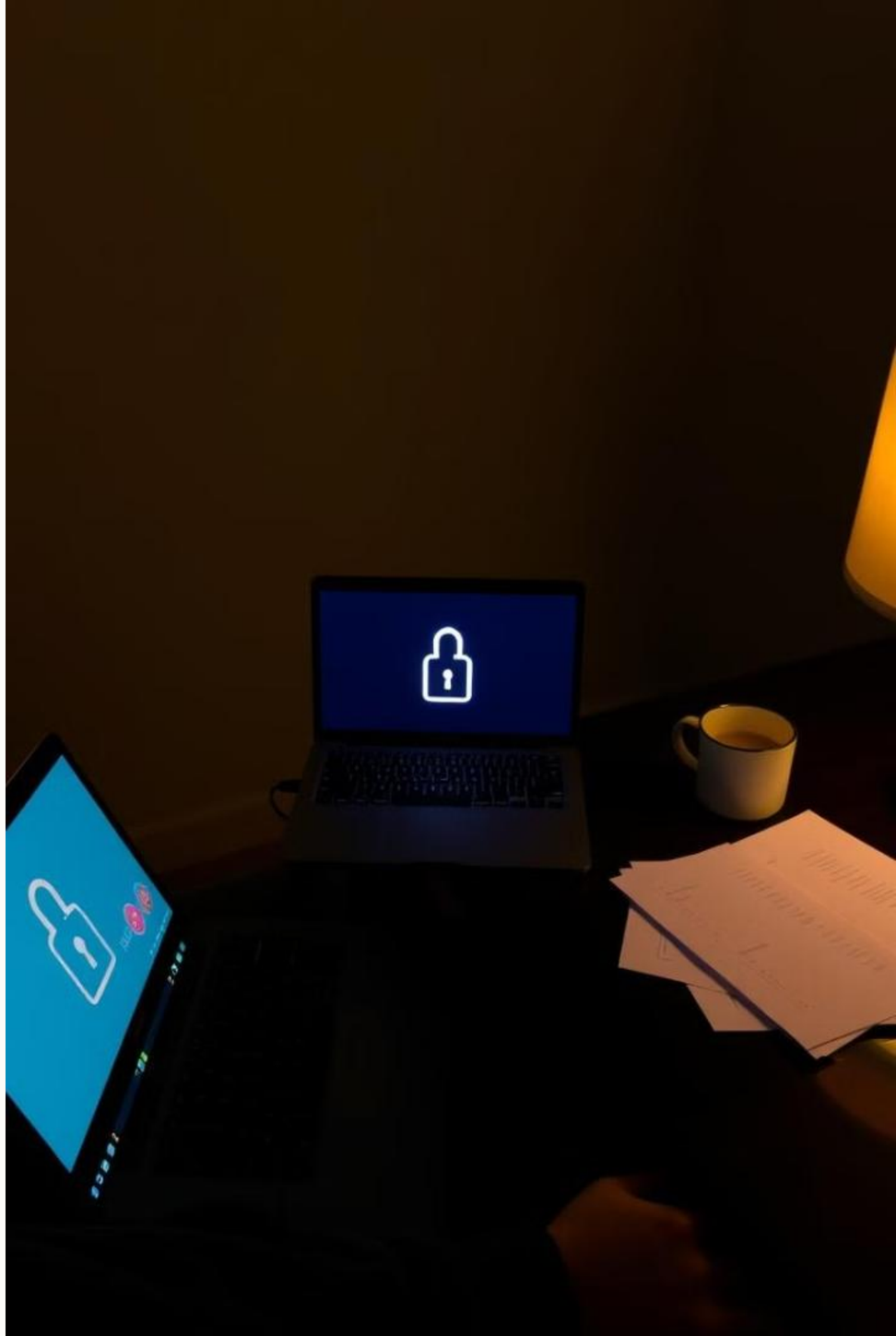
# Bezpieczeństwo w Internecie: Jak Unikać Przestępstw Online

Internet stanowi przestrzeń bogatą w możliwości, ale jednocześnie niesie ze sobą liczne zagrożenia. Przestępcy wykorzystują tę sieć do kradzieży danych, pieniędzy oraz tożsamości. Ta prezentacja ma na celu podniesienie świadomości na temat niebezpieczeństw związanych z aktywnością w sieci oraz zaprezentowanie praktycznych metod ochrony przed nimi.



# Najczęstsze Rodzaje Przestępstw Internetowych

## Phishing

Fałszywe e-maile lub strony internetowe, które próbują wyłudzić dane osobowe lub finansowe.

## Malware

Złośliwe oprogramowanie, takie jak wirusy i trojany które mogą uszkodzić komputer lub ukraść dane.

## Kradzież Tożsamości

Nielegalne wykorzystanie cudzych danych osobowych do uzyskania korzyści finansowych lub innych.

## Fałszywe Sklepy Internetowe

Strony internetowe udające sklepy, które oferują towary po bardzo niskich cenach, ale nie dostarczają towarów ani nie zwracają pieniędzy.

# Bezpieczne Zakupy i Bankowość Online

1. Sprawdzaj wiarygodność sklepów internetowych. Szczególną uwagę zwróć na adres internetowy, opinie i dane kontaktowe.

2. Korzystaj z bezpiecznych metod płatności, takich jak karty wirtualne, systemy płatności (np. PayPal) i unikaj przelewów bezpośrednich.

3. Postępuj ostrożnie z ofertami i promocjami. Podejrzanie niskie ceny mogą wskazywać na oszustwo.

4. Zabezpieczaj komputer i sieć. Używaj aktualnego programu antywirusowego i bezpiecznego połączenia Wi-Fi.

# Ochrona Prywatności w Mediach Społecznościowych

Ustawienia prywatności: Ogranicz widoczność profilu i kontroluj udostępniane informacje.

Uważność na udostępniane treści: Unikaj publikowania wrażliwych danych i zdjęć z lokalizacją.

Ochrona przed stalkingiem: Blokuj osoby, zgłaszaj nadużycia i skontaktuj się z policją w razie zagrożenia.

Phishing w mediach społecznościowych: Rozpoznawaj fałszywe linki i wiadomości.

# Podsumowanie i Dalsze Kroki

1. Zawsze bądź ostrożny w sieci. Używaj silnych haseł, zabezpieczaj swoje urządzenia i nie udostępniaj wrażliwych danych.

2. Śledź nowości i aktualizuj wiedzę na temat zagrożeń. Korzystaj ze źródeł informacji, takich jak CERT Polska, policja i organizacje zajmujące się bezpieczeństwem w internecie.

3. Zadawaj pytania, jeśli masz wątpliwości. Zawsze lepiej dmuchać na zimne niż ponieść szkody.