



**fundacja instytut**  
**CYBERBEZPIECZEŃSTWA**

**Fałszywe strony,  
prawdziwe straty,  
czyli jak nie dać się  
oszukać?**

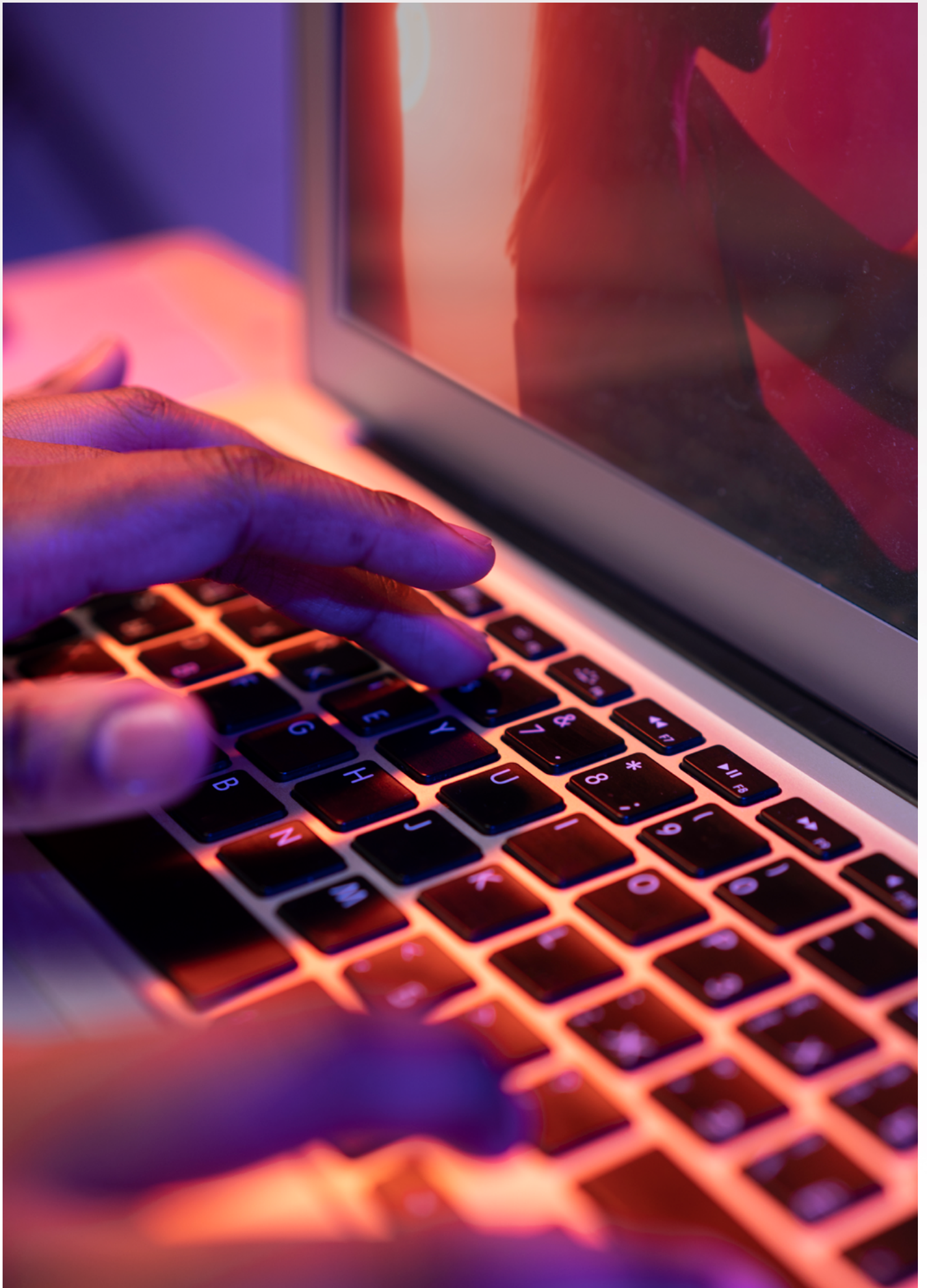


Fundusz  
Sprawiedliwości



Ministerstwo  
Sprawiedliwości

Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości



Współczesna cyberprzestrzeń oferuje nam natychmiastowy dostęp do różnych źródeł informacji oraz umożliwia swobodną komunikację w czasie rzeczywistym z ludźmi z całego świata. Ułatwia pracę, naukę, zakupy i korzystanie z wielu usług bez wychodzenia z domu. Jednocześnie zapewnia niemal nieograniczone możliwości rozrywki, takie jak gry, filmy, muzyka oraz wirtualne wydarzenia, np. webinary czy webcasty. Mimo dobrodziejstw, jakie oferuje nam korzystanie z internetu, należy pamiętać, że wiąże się to również z licznymi zagrożeniami.

Zespół CERT Polska odnotował, że liczba zarejestrowanych incydentów cyberbezpieczeństwa w październiku tego roku wyniosła 40,1 tys. W porównaniu z analogicznym miesiącem w roku poprzednim (2024) oznacza to wzrost aż o 375%. Należy podkreślić, że 39,4 tys. z tych incydentów (98%) zaklasyfikowano do zagrożeń określanych mianem „oszustw komputerowych”. Ponadto od stycznia do października 2025 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami<sup>1</sup> wpisano łącznie 197,5 tys. szkodliwych domen. Warto dodać, że w samym październiku 2025 r. pojawiło się tam 36,9 tys. nowych nazw domen wykorzystywanych do wyłudzenia danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych.

Wartość zwiększyła się o 46% w stosunku do miesiąca poprzedniego (25,2 tys.)<sup>2</sup>. Z tego względu konieczne jest zachowanie czujności i wdrożenie kilku zasad, które pozwolą nam skutecznie chronić się przed zagrożeniami tego typu.

Przed wszystkim należy zawsze zwracać uwagę na adres URL (ang. Uniform Resource Locator) strony internetowej. Fałszywe witryny często wykorzystują nieznacznie zmienione adresy, dodatkowe znaki lub nietypowe domeny, które na pierwszy rzut oka mogą wydawać się prawidłowe. Oszuści wykorzystują metodę zwaną *typosquatting*. Polega ona na rejestracji domen zawierających częste błędy popełniane przez użytkowników przy wpisywaniu adresów w pasku adresu, czyli np. literówki. Po wpisaniu takiego błędnego adresu (np. zamiast „allegro.pl” -> „allegor.pl”) użytkownik może trafić na stronę przypominającą tę oryginalną, na której atakujący próbują wyłudzić dane logowania lub inne wrażliwe informacje. Inną metodą jest wykorzystanie znaków do złudzenia przypominających te użyte w prawdziwym adresie. Przykładem może być wykorzystanie liter z cyrylicy udających łacińskie „a” czy „o”, co pozwala na tworzenie domen wyglądających identycznie dla osoby niezwracającej uwagi na szczegóły. Warta wspomnienia jest również sytuacja

1 Lista Ostrzeżeń przed niebezpiecznymi stronami, CERT.PL, <https://cert.pl/lista-ostrzezen/>; (dostęp: 16.11.2025)

2 Raport: Podsumowanie Miesiąca Cert POLSKA / CSIRT NASK nr 2/2025 [https://cert.pl/uploads/docs/Podsumowanie\\_CSIRT\\_NASK\\_2025\\_10.pdf](https://cert.pl/uploads/docs/Podsumowanie_CSIRT_NASK_2025_10.pdf); (dostęp: 16.11.2025)

jedno z użytkowników portalu społecznościowego Reddit. Otrzymał on e-mail wyglądający jak wiadomość od Microsoftu z prośbą o zresetowanie hasła oraz odnośnikiem do strony internetowej. Wszystkie elementy wydawały się autentyczne. Logo, układ i treść były niemal identyczne względem wyglądu oficjalnej korespondencji. Dopiero po chwili odbiorca zauważył, że nadawca to „noreply@rnicrosoft.com. Litery „r” i „n” były ustawione obok siebie, tworząc iluzję litery „m”, co sprawiało wrażenie prawdziwego adresu Microsoftu<sup>3</sup>. Jest to przykład tzw. *homograph scam*, w którym oszust wykorzystuje podobnie wyglądające znaki, przypominające litery zawarte w oryginalnych adresach. Otrzymując podejrzaną wiadomość, warto również dokładnie sprawdzić linki i przyciski. Zanim klikniemy odnośnik, dobrze jest najechać na niego kursorem i zwrócić uwagę na adres URL wyświetlany w dolnej części przeglądarki, który często ujawnia prawdziwy kierunek przekierowania. Ostrożność jest szczególnie wskazana w przypadku tzw. skraccaczy URL lub linków o nietypowej strukturze, które mogą prowadzić do stron podszywających się pod znane serwisy.

Rozpoznanie fałszywej strony internetowej możliwe jest również dzięki uważnemu przeanalizowaniu jej wyglądu. Warto zwracać uwagę na elementy wizualne i treść.

Dla użytkownika sygnałem ostrzegawczym powinny być błędy językowe, literówki oraz nieudane tłumaczenia. Niska jakość oprawy graficznej, w tym elementów identyfikacji wizualnej danej instytucji, w tym szczególnie brak spójności powinien zwrócić naszą uwagę. Fałszywe witryny często stosują mechanizmy wywołujące presję i pośpiech u użytkownika. Typowe przykłady to komunikaty o pilnej płatności, informacje o rzekomych problemach z kontem lub groźby utraty dostępu do usług. Nietypowe okna logowania lub formularze proszące o wprowadzenie wrażliwych danych, które nie wyglądają jak standardowe formularze znanych usług, w szczególności powinny wzbudzić naszą wątpliwość. Ponadto brak regulaminu, danych kontaktowych czy polityki prywatności jest kolejnym sygnałem, że witryna może być niebezpieczna i niegodna zaufania. Oczywiście, należy także sprawdzić, czy strona korzysta z protokołu HTTPS, co w przeglądarce oznacza ikonę kłódki obok adresu URL. Dzięki temu, połączenie jest szyfrowane przy użyciu TLS, a przesyłane dane, są chronione przed przechwyceniem przez osoby trzecie. Trzeba jednak pamiętać, że oszuści mogą łatwo zdobyć taki certyfikat, więc kłódka oznacza tylko, że połączenie jest szyfrowane, ale nie gwarantuje, że strona jest bezpieczna. Skutecznym sposobem ochrony jest używanie menedżerów haseł, zwłaszcza tych

3 User gets a password reset mail from rnicrosoft.com, everything looks fine until he spots a chilling deception (2025) *The Economic Times* <https://economictimes.indiatimes.com/news/new-updates/user-gets-a-password-reset-mail-from-rnicrosoft-com-everything-looks-fine-until-he-spots-a-chilling-deception/articleshow/124738647.cms>; (dostęp: 16.11.2025)



połączonych z przeglądarką i oferujących automatyczne wypełnianie danych logowania (np. Keepass, który można zintegrować z przeglądarką). Dzięki temu nawet jeśli użytkownik trafi na stronę podszywającą się pod prawdziwą witrynę, program nie wprowadzi zapisanych haseł na fałszywej domenie. Warto korzystać z zaufanych, sprawdzonych rozwiązań, które zapewniają wysoki poziom ochrony danych.

Podsumowując, w obliczu gwałtownego wzrostu skali cyberataków oraz coraz bardziej wyrafinowanych metod oszustów, kluczowe staje się rozwijanie świadomości i umiejętności krytycznego myślenia. Internet nie jest przestrzenią całkowicie bezpieczną, lecz staje się znacznie mniejszym

zagrożeniem, gdy korzystamy z niego uważnie, analizujemy otrzymywane komunikaty i nie działamy pod wpływem presji. Stosowanie podstawowych zasad ostrożności, takich jak sprawdzanie adresów URL, analizowanie wyglądu strony czy korzystanie z menedżerów haseł – pozwala znacząco ograniczyć ryzyko utraty danych. Warto również pamiętać, że bezpieczeństwo jest procesem wymagającym stałej czujności i aktualizowania wiedzy. Tylko świadome korzystanie z technologii, połączone z odpowiedzialnymi nawykami, może skutecznie chronić nas przed dynamicznie zmieniającymi się zagrożeniami w świecie cyfrowym.

## Źródła:

- Lista Ostrzeżeń przed niebezpiecznymi stronami, CERT.PL, <https://cert.pl/lista-ostrzezen/>; (dostęp: 16.11.2025)
- Raport: Podsumowanie Miesiąca Cert POLSKA / CSIRT NASK nr 2/2025 [https://cert.pl/uploads/docs/Podsumowanie\\_CSIRT\\_NASK\\_2025\\_09.pdf](https://cert.pl/uploads/docs/Podsumowanie_CSIRT_NASK_2025_09.pdf); (dostęp: 16.11.2025)
- User gets a password reset mail from rnicrosoft.com, everything looks fine until he spots a chilling deception (2025) The Economic Times [https://economictimes.indiatimes.com/news/new-updates/user-gets-a-password-reset-mail-from-rnicrosoft-com-everything-looks-fine-until-he-spots-a-chilling-deception/articleshow/124738647.cms?utm\\_source=contentofinterest&utm\\_medium=text&utm\\_campaign=cppst](https://economictimes.indiatimes.com/news/new-updates/user-gets-a-password-reset-mail-from-rnicrosoft-com-everything-looks-fine-until-he-spots-a-chilling-deception/articleshow/124738647.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst) (dostęp: 16.11.2025)



# **fundacja instytut**

## **CYBERBEZPIECZEŃSTWA**



**[www.instytutcyber.pl](http://www.instytutcyber.pl)**



Fundusz  
Sprawiedliwości



Ministerstwo  
Sprawiedliwości

Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości