

## Dział Organizacji Zasobów Informacyjnych

Warszawa, dnia 9 maja 2025 roku

### UWAGA PHISHING – ZACHOWAJ OSTROŻNOŚĆ!

*Szanowni Państwo,*

przypominamy o konieczności zachowania szczególnej ostrożności w związku z rosnącą liczbą kampanii phishingowych wymierzonych w użytkowników uczelnianej poczty elektronicznej.

#### Czym jest phishing?

Phishing to metoda oszustwa polegająca na podszywaniu się pod zaufane osoby lub instytucje (np. uczelnie wyższe, administrację publiczną, banki, działy IT) w celu wyłudzenia poufnych danych, takich jak loginy, hasła, dane osobowe czy informacje finansowe. Ataki te najczęściej realizowane są za pośrednictwem fałszywych wiadomości e-mail, SMS lub stron internetowych.

*Więcej o phishingu:*

<https://odo.uw.edu.pl/wp-content/uploads/sites/10/2020/07/Phishing.pdf>

#### Jak bronić przed phishingiem?

- **uwaga**nie czytaj otrzymaną korespondencję – zwracaj uwagę na podejrzaną linki, błędy językowe, nietypowe adresy nadawców;
- **nie** klikaj w nieznane linki ani **nie** otwieraj załączników od podejrzanych nadawców.
- **nie** podawaj danych logowania ani danych osobowych w odpowiedzi na wiadomości e-mail;
- **sprawdź** adresy stron internetowych – upewnij się, że adres jest prawidłowy i nie zawiera żadnych literówek lub nietypowych znaków;
- **nie** podawaj danych logowania ani danych osobowych na podejrzanej stronie internetowej;
- **zgłaszaj** wszelkie podejrzaną wiadomości do Inspektora Ochrony Danych, Zespołu Bezpieczeństwa Teleinformatycznego lub informatyka w jednostce organizacyjnej.

#### Gdzie zgłaszać phishing?

Podejrzaną wiadomości prosimy zgłaszać do:

- ⇒ Inspektor Ochrony Danych: [iod@adm.uw.edu.pl](mailto:iod@adm.uw.edu.pl)
- ⇒ Zespół Bezpieczeństwa Teleinformatycznego: [abuse@uw.edu.pl](mailto:abuse@uw.edu.pl)

---

**PAMIĘTAJ:** Należy zachować ostrożność – jedna nieuwważna decyzja może narazić pracownika oraz całą Uczelnię na konsekwencje.

## Przykładowe wiadomości phishingowe:

**Wzmożone ataki phishingowe**

• Mailing <jd429182@students.mimuw.edu.pl> Yesterday at 13:44

Szanowni Państwo,

w ostatnim czasie, jak zapewne Państwo zauważyli, obserwujemy wzmożoną liczbę ataków phishingowych. W związku z tym chcielibyśmy uczulić Państwa na konieczność dokładnego sprawdzania otrzymywanych wiadomości.

Do najczęstszych cech wiadomości phishingowych należą:

- podszywanie się pod inne osoby (np. nadawca podpisuje się jako „Rektor UW” lub „Sekcja IT”, choć adres wskazuje na „Jan Kowalski”),

Zwracamy się z prośbą o pomoc w zablokowaniu wszelkich prób phishingu na Państwa pocztę elektroniczną oraz na pocztę elektroniczną całego uniwersytetu.

Jeżeli nie podejmiesz żadnych działań, konto zostanie zablokowane i nie będziesz mieć dostępu do poczty e-mail ani żadnych aplikacji uniwersyteckich.

W ramach naszej usługi, aby uniknąć: prosimy o ponowne połączenie z dostępem poprzez kliknięcie [zabezpiecz mój e-mail](#)

Jeśli mają Państwo podejrzenie, że mogli paść ofiarą takiego ataku, zalecamy niezwłoczną zmianę hasła do USOS oraz poczty.

W razie jakichkolwiek wątpliwości służymy pomocą — zapraszamy do kontaktu:

*Annotations:*  
falszywy adres e-mail  
wykorzystanie faktycznego zdarzenia  
niespójne lub nietypowe formatowanie tekstu  
link do strony www spoza UW

**Ważne informacje: Incydent IT Awarii w Twojej uniwersyteckiej poczcie e-mail**

MK [redacted] <[redacted]@wpia.uw.edu.pl> Wednesday, 7 May 2025 at 15:34

To: (wielu adresatów)

Drodzy wszyscy,

Informujemy, że atak phishingowy ma obecnie wpływ na usługi poczty elektronicznej uczelni, powodując awarie mogące utrudniać korzystanie z nich. Nasze zespoły techniczne są w pełni zmobilizowane, aby zidentyfikować źródło problemu i przywrócić usługę tak szybko, jak to możliwe. Zwracamy się z prośbą o pomoc w zablokowaniu wszelkich prób phishingu na Państwa pocztę elektroniczną oraz na pocztę elektroniczną całego uniwersytetu.

Jeżeli nie podejmiesz żadnych działań, konto zostanie zablokowane i nie będziesz mieć dostępu do poczty e-mail ani żadnych aplikacji uniwersyteckich.

W ramach naszej usługi, aby uniknąć: prosimy o ponowne połączenie z dostępem poprzez kliknięcie [zabezpiecz mój e-mail](#)

Będziemy informować Państwa o rozwoju sytuacji.

Przepraszamy za wszelkie niedogodności.

Dział IT

*Annotations:*  
nadawca niespójny z podpisem  
link do strony www spoza UW