UNIWERSYTET WARSZAWSKI

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?

- **uważnie czytaj otrzymaną korespondencję** – zwracaj uwagę na podejrzane 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;
- **sprawdzaj 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 podejrzane wiadomości** do Inspektora Ochrony Danych, Zespołu Bezpieczeństwa Teleinformatycznego lub informatyka w jednostce organizacyjnej.

Gdzie zgłaszać phishing?

Podejrzane wiadomości prosimy zgłaszać do:

⇒ Inspektor Ochrony Danych: iod@adm.uw.edu.pl
⇒ Zespół Bezpieczeństwa Teleinformatycznego: abuse@uw.edu.pl

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

ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa
tel.: 22 55 22 042
e-mail: iod@adm.uw.edu.pl

Przykładowe wiadomości phishingowe: