Bezpieczny e-mail: Mikro-poradnik

• Adres e-mail: Niestety adresy nadawców są bardzo łatwe do sfałszowania. Z podejrzliwością należy podchodzić do każdego e-maila, jeśli jego nadawca nie należy do instytucji, z której rzekomo pochodzi (dobrze jest znać nazwiska prowadzących zajęcia i nazwiska osób z dziekanatu i instytutu zajmujących się dydaktyką).

• Treść wiadomości e-mail: jak wiarygodna jest treść? Słaba znajomość języka polskiego, nielogiczna argumentacja, nietypowe prośby są zawsze oznaką, że coś jest nie tak. Jeśli masz wątpliwości, zapytaj – ale nigdy nie korzystaj z danych kontaktowych z poczty elektronicznej, zamiast tego skorzystaj z alternatywnego źródła (książka telefoniczna, własne kontakty e-mailowe, Internet).

• Linki internetowe: Jeśli podejrzana wiadomość e-mail zawiera łącze, nigdy jej nie otwieraj przed sprawdzeniem jej autentyczności – po prostu najedź na nią myszką, aby wyświetlić adres URL: Jeśli adres URL wskazuje domenę, która nie pasuje do domniemanego nadawcy, jest to bardzo mocny znak złego postępowania. Domena politechniczna to …@**put.poznan.pl**. Maile od pracowników Instytutu Informatyki mogą również pochodzić z poddomeny @**cs.put.poznan.pl**. Należy pamiętać, że napastnicy czasami próbują sprawić, aby adres URL wyglądał prawie jak oryginalna domena rzekomego nadawcy.

• Certyfikat SSL: Jeśli adres URL zaczyna się od https://, jest to połączenie szyfrowane. Nigdy nie podawaj wrażliwych danych żadnej witrynie internetowej, która nie korzysta z protokołu HTTPS. Nowoczesne przeglądarki internetowe wskażą prawidłowe szyfrowanie ikoną kłódki.

• Nie podążaj za adresami URL (linkami) bezpośrednio zawartymi w wiadomości e-mail.

• Nie daj się nabrać na presję e-maili i nie ulegaj pokusie szybkiego działania bez zastanowienia.

• W przypadku próśb i zapytań kierowanych drogą e-mailową, w pierwszej kolejności sprawdź nadawcę i w razie wątpliwości skontaktuj się z nim innym kanałem komunikacji (np. telefonem). Jeszcze raz: nie daj się nabrać na presję e-maila.

• Mail address: Unfortunately, sender addresses are very easy to forge. You should be suspicious of any e-mail if its sender does not belong to the institution from which it claims to originate.

• Mail content: How credible is the content? Poor English, illogical argumentation, unusual requests are always an indication that something is wrong. If in doubt, ask - but never use contact data from the e-mail, instead use an alternative source (telephone book, own e-mail contacts, web).

• Web Links: If the suspicious email contains a link, never open it before verifying its authenticity – just move your mouse over it to view the URL: If the URL points to a domain that does not match the alleged sender, it is a very strong sign of wrongdoing. Please note that

attackers sometimes try to make the URL look almost like the original domain of the supposed sender.

• SSL certificate: If the URL starts with https:// it is an encrypted connection. Never give sensitive data to any website that is not using HTTPS. Modern web browsers will indicate proper encryption with a lock icon.

• Do not follow URLs (links) directly in an e-mail.

• Do not let yourself be pressured by an e-mail and be tempted to act quickly without thinking.

• In the case of requests and inquiries via e-mail, first check the sender and, if in doubt, contact them via another communication channel (e.g.: telephone). Again, do not let yourself be pressured by the e-mail.

--- ---