

Korespondencja online to nie tylko maile i przekazywane w nich załączniki, ale także wszystkie rozmowy, które prowadzimy przez serwisy społecznościowe, komunikatory i inne aplikacje umożliwiające wysyłanie wiadomości.

Eksperti zajmujący się cyberbezpieczeństwem przypominają, że podstawą naszej ochrony w świecie online są silne hasła, za pomocą których logujemy się do różnych serwisów internetowych oraz skrzynek pocztowych. Co bardzo ważne, powinniśmy znać je tylko my. Aby stworzyć silne hasło, należy zachować trzy najważniejsze zasady. Po pierwsze: silne hasło to długie hasło, po drugie: łatwo je zapamiętać, ale trudno odgadnąć, wreszcie po trzecie: jest unikalne dla każdej usługi, z której korzystamy.

Kolejna podstawowa zasada o jakiej należy pamiętać to zwrócenie uwagi na wiadomości phishingowe i inne kampanie przygotowywane przez cyberprzestępców, które można otrzymać na skrzynkę e-mail, jak również przez komunikatory i wiadomości SMS.

Zawsze należy zwracać uwagę na nadawcę – nie odczytywać wiadomości od nieznajomych, zwłaszcza gdy mamy wrażenie, że ktoś podszywa się pod firmę, instytucję lub inną osobę. Nigdy nie należy klikać w załączniki i linki przesyłane przez nieznaną nadawców – mogą zawierać szkodliwe oprogramowanie.

Ponadto, Nigdy nie należy udostępniać haseł, danych logowania, danych do karty płatniczej lub kodów BLIK innym osobom. Kolejna ważna zasada to nie korzystanie z prywatnych komputerów do celów służbowych i odwrotnie.

Wysyłając wiadomości online trzeba mieć świadomość, że mogą one trafić w niepowołane ręce. Coraz więcej usług gwarantuje szyfrowanie wiadomości. Mimo to, warto zachować szczególną ostrożność, zwłaszcza gdy udostępniamy informacje poufne.

Pamiętać należy aby nigdy nie wysyłać ważnych danych (np. numeru PESEL, czy haseł dostępu) bez dodatkowego szyfrowania. Jeśli musimy je komuś przekazać, nie róbmy tego w jednej wiadomości e-mail, tylko za pomocą mieszanych kanałów komunikacji – np. hasło do zaszyfrowanego pliku prześlij SMS-em.

*Źródło: [MC](#)*