Bezpieczna poczta e-mail – to trzeba wiedzieć!

E-mail to jedna z najpopularniejszych form komunikacji internetowej. Adres poczty elektronicznej to także identyfikator, którego używamy w trakcie logowania do różnych serwisów online. Dlatego warto wiedzieć, jak zadbać o bezpieczeństwo swojej poczty. Podpowiadamy, jak to zrobić.

Skrzynki poczty elektronicznej to jedno z najczęściej atakowanych przez cyberprzestępców narzędzi. Skutki takich działań dotykają coraz większej liczby osób. Warto zatem poznać sposoby, jak utrudnić życie cyberprzestępcom i zapewnić sobie bezpieczeństwo. To nic trudnego!

Silne hasło na początek

Mailujemy w pracy, do znajomych, na maila dostajemy swoje rachunki i ważne informacje, np. z banku. Swój adres e-mail podajemy logując się do mediów społecznościowych, sklepów internetowych, rozpoczynając subskrypcję w serwisach streamingowych i w wielu innych miejscach.

Dlatego w naszych skrzynkach e-mailowych lądują ważne informacje i dane, często wrażliwe. Ich wykradzenie może nas dużo kosztować. Dlatego warto zrobić wszystko, by tego uniknąć. Jak to zrobić? Postępuj zgodnie z naszymi wskazówkami.

Od czego zacząć? - Eksperci cyberbezpieczeństwa są zgodni - silne hasło to podstawa naszego bezpieczeństwa w cyfrowym świecie. Stosując się do kilku prostych zasad przy tworzeniu haseł jesteśmy w stanie minimalizować ryzyko ich złamania – mówi minister Janusz Cieszyński, pełnomocnik rządu ds. cyberbezpieczeństwa.

Na początek trzy zasady:

Silne hasło jest długie - długość hasła ma największe znaczenie. Im więcej znaków do odgadnięcia, tym trudniejsze zadanie dla cyberprzestępcy i jego narzędzi. Hasło powinno mieć co najmniej 8 znaków. Jeszcze lepsze jest dłuższe hasło, składające się z 12 lub 14 znaków.

Łatwo je zapamiętać, ale trudno odgadnąć - nietrudno wymyślić długie hasło mające ponad 20 znaków, ale z zapamiętaniem go możesz już mieć niemały problem. Dlatego ważne jest, by dobrze to sobie przemyśleć. Tworząc hasło - zadbaj, by z czymś ci się kojarzyło. Równocześnie jednak postaraj się o to, aby trudno było je odgadnąć. Dobrze, by w swojej treści zawierało coś, o czym wiesz tylko Ty i co tylko Ty zrozumiesz.

Dobre hasło wykorzystujesz tylko w jednej usłudze! Nigdy nie powtarzaj swojego hasła w kilku serwisach internetowych. W każdym serwisie internetowym korzystaj z innego hasła!

Więcej wskazówek o tym jak utworzyć bezpieczne hasło znajdziesz w naszym artykule.

Masz już silne hasło - czy w końcu możesz odetchnąć z ulgą? Niekoniecznie... Nawet długi i skomplikowany ciąg znaków nie zabezpieczy nas, jeśli zapiszemy go na karteczce i przykleimy do monitora. Najważniejsze to nie ujawniać nikomu swojego hasła. Od czasu do czasu hasło też trzeba zmieniać. A jak już zmieniamy hasło, to na pewno nie z Ja$2016 na Ja$2017.

Co jeszcze możesz zrobić?

Hasło to nie wszystko. Jeśli chcesz, aby Twoja poczta elektroniczna była bezpieczna, pamiętaj jeszcze o tym:

Dwustopniowa weryfikacja - często teraz słyszymy o przejętych, zaatakowanych kontach, wykradzionych hasłach czy wyciekach danych. Warto więc zainteresować się dwustopniowym uwierzytelnianiem. Ta funkcjonalność znacznie zwiększa bezpieczeństwo naszego konta. Jak? Przez dodanie do logowania dodatkowego czynnika uwierzytelniającego

naszą tożsamość. To może być np. jednorazowy kod przesłany smsem.

Więcej o dwustopniowej weryfikacji w zajedziesz w naszym artykule Dwa składniki, czyli przepis na cyberbezpieczeństwo.

Publiczne sieci Wi-Fi - korzystając z otwartej sieci Wi-Fi powinniśmy być szczególnie ostrożni. W takiej sytuacji, jeśli to możliwe, nie logujmy się do poczty e-mail. Przeczytaj nasze porady dotyczące bezpiecznego korzystania z internetu poza domem.

Rozważ korzystanie z kilku skrzynek pocztowych - mailem często logujemy się do różnych serwisów internetowych, w tym mediów społecznościowych. Choć korzystanie z tylko jednego adresu może być wygodne, to przy przejęciu danych do logowania, cyberprzestępca uzyskuje też dostęp do powiązanych z nim usług. Dlatego warto korzystać z kilku adresów w różnych serwisach. Po to, że gdyby okazało się, że staliśmy się ofiarą cyberataku – nie stracić wszystkiego za jednym razem.

Odpowiadanie na podejrzane wiadomości - do oszustw za pośrednictwem poczty e-mail wykorzystywane są przede wszystkim ataki typu phishing. Stosujący go cyberprzestępcy wykorzystują znaną technikę, która ma spowodować, że podejmiemy działania zgodne z ich zamierzeniami. To dlatego kuszą nas sensacyjnymi tytułami, niepowtarzalnymi ofertami, czy promocjami. Dlatego warto być szczególnie wyczulonym na wiadomości, które wzbudzają naszą nawet najmniejszą wątpliwość. Pamiętaj, by nigdy w żadnej wiadomości nie podawać swoich haseł, numerów kart płatniczych, czy jakichkolwiek innych wrażliwych informacji. Żadna instytucja, ani żaden bank, nigdy nie poprosi Cię o takie informacje drogą elektroniczną.

Dowiedz się więcej, jak chronić się przed phishingiem?

Jak rozpoznać fałszywy e-mail?

Oto kilka pytań, na które warto odpowiedzieć, zanim otworzysz i odpowiesz na wiadomość e-mail:

Czy znasz nadawcę wiadomości? Jeśli uważasz, że znasz nadawcę, sprawdź dokładnie aktualny adres e-mail. Często wiadomość e-mail wyłudzająca informacje będzie pozornie wyglądać tak, jakby pochodziła od osoby lub instytucji, którą znasz. Różnica? To może być np. niewielka zmiana w adresie.
Czy otrzymałaś/-eś już inne wiadomości od tego nadawcy?
Czy spodziewałaś/-eś się otrzymać tę wiadomość?
Czy tytuł wiadomości i nazwa załącznika mają sens? Czy wiadomość nie zawiera złośliwego oprogramowania – jaki jest wynik skanowania antywirusowego?

Jeśli na któreś z tych pytań odpowiedź brzmi: nie - uważaj.

O czym jeszcze warto pamiętać?

Nie należy używać prywatnych kont poczty elektronicznej do korespondencji służbowej, a także prywatnych komputerów i telefonów do spraw służbowych. Każdy pracownik powinien wyraźnie oddzielać e-maile prywatne od firmowych. W przypadku przejęcia skrzynki poczty elektronicznej przez cyberprzestępców jesteśmy narażeni na wyciek nie tylko naszych prywatnych informacji, ale również danych firmy.

Reaguj! Wszystkie podejrzane wiadomości na prywatnej skrzynce można zgłosić do CSIRT NASK wysyłając maila na adres incydent.cert.pl lub cert@cert.pl

Dodatkowo, CSIRT NASK przygotował zbiór zasad dotyczących bezpiecznego korzystania z poczty elektronicznej i mediów społecznościowych. Warto je poznać – koniecznie przeczytaj!

Bądźcie bezpieczni podczas korzystania z poczty elektronicznej i pamiętajcie, że najsłabszym ogniwem zawsze (niestety) jest jej użytkownik! Nie dajcie się cyberprzestępcom!

Informacja MC