OUCH! | Kwiecień 2017

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- **Dobre hasła**
- **Bezpieczne korzystanie z haseł**
- **Baza wiedzy**

Dobre hasła

Czym są hasła

Hasła są wykorzystywane każdego dnia. Używasz ich logując się do poczty, bankowości internetowej, robiąc zakupy on-line czy odblokowując smartfona. Hasła to także jeden z krytycznych punktów ochrony prywatności. Jeśli ktokolwiek powtórzy, lub odgadnie Twoje hasło, może uzyskać dostęp do Twojego konta w banku, przeczytać Twoje maile, lub ukraść Twoją tożsamość. To dlatego silne hasła są podstawą skutecznej ochrony. Wiemy, że hasła bywają kłopotliwe, są trudne do zapamiętania, i sprawiają problem przy wpisywaniu. Dlatego w tym numerze postaramy nauczyć Cię tworzenia silnych haseł, które są proste do zapamiętania oraz łatwe do wprowadzania.

Redaktor gościnny

My-Ngoc Nguyen (znana również jako Me-Nop Wynn) jest certyfikowanym instruktorem SANS oraz głównym konsultantem ds. bezpieczeństwa IT. Posiada 15-letnie doświadczenie w tworzeniu, implementacji oraz zarządzaniu programami bezpieczeństwa dla wielu przedsiębiorstw oraz organizacji. Można znaleźć ją na Twitterze (**@MenopN**) oraz na LinkedIn: My-Ngoc “Menop” Nguyen

Silne hasła

Przestępcy komputerowi opracowali skuteczne sposoby automatycznego odgadywania haseł. Na złamanie (ang. bruteforcing) szczególnie są narażone proste hasła. Pamiętaj, że używanie silnych haseł podnosi poziom Twojego bezpieczeństwa. Dobre hasło powinno stanowić nieszablonową kombinację znaków lub wyrazów. Niestety, często skomplikowane hasła są trudne do zapamiętania, a ich wprowadzanie mało wygodne. Alternatywą jest użycie haseł będących serią losowych słów lub zdaniem. Im więcej znaków posiada hasło, tym jest ono trudniejsze do złamania. Zaletą tak dobranego hasła jest o wiele bardziej intuicyjne wprowadzanie oraz łatwiejsze zapamiętywanie, przy czym tego typu hasło jest trudne do złamania przez przestępców. Poniżej prezentujemy dwa różne przykłady:

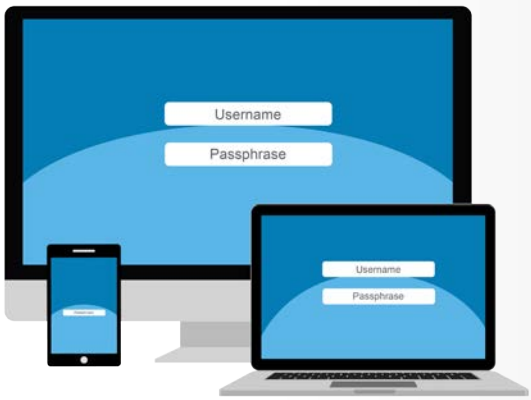
Litwo!Ojczyzno moja!
B3zpi3czneHa$l0_1337

Powyższe hasła są silne ponieważ są nie tylko długie, ale również zawierają wielkie litery oraz znaki specjalne (spację oraz znak “!”). Jednocześnie są one łatwe do zapamiętania. Hasło może być jeszcze trudniejsze do złamania po dokonaniu zamiany części liter na znaki lub cyfry np. litery “o” na cyfrę “0”, co przedstawiono w drugim przykładzie. Jeśli oprogramowanie lub strona internetowa posiada ograniczenie długości hasła, staraj się wykorzystać maksymalną ilość dostępnych znaków.

Dobre hasła

Bezpieczne używanie haseł

Nawet używając skomplikowanych haseł, zawsze należy zachować ostrożność. Użycie silnego hasła nie gwarantuje pełnego bezpieczeństwa, jeśli przestępcy będą w stanie łatwo je wykraść lub skopiować.



Hasła oparte na całych frazach są bardzo skutecznym sposobem na stworzenie i zapamiętanie silnych haseł.

1. Zawsze staraj się używać różnych haseł dla posiadanych kont oraz urządzeń. Nigdy nie używaj tego samego hasła do komputera w pracy, konta bankowego oraz kont na prywatnych portalach społecznościowych jak Facebook, Youtube czy Twitter. Dzięki temu, jeśli przestępcom uda się uzyskać dostęp do jednego z kont, pozostałe nadal będą bezpieczne. Jeśli masz zbyt wiele kont i nie jesteś w stanie zapamiętać wszystkich haseł, rozważ użycie menedżera haseł. Jest to oprogramowanie specjalnie zaprojektowane do bezpiecznego przechowywania dostępów do kont. Dzięki niemu będziesz musiał zapamiętać jedynie dwa hasła: jedno do zalogowania się na komputerze oraz drugie do menedżera haseł.
2. Nigdy nie dziel się z innymi, także przełożonymi czy współpracownikami, swoim hasłem lub metodą jego tworzenia. Traktuj hasło jak sekret, jeśli ktokolwiek je zna, hasło nie jest już bezpieczne. Jeśli przez przypadek udostępnisz komuś swoje hasło lub podejrzewasz, że mogło zostać wykradzione, jak najszybciej je zmień. Jedynym wyjątkiem jest wyjątkowa sytuacja, w której chcesz udostępnić hasło zaufanej, bliskiej osobie. Jednym podejściem rozwiązania tej sytuacji jest zapisanie kluczowego hasła, umieszczenie go w bezpiecznym miejscu i udostępnienie jego lokalizacji zaufanej osobie. W takim przypadku, jeśli wydarzy się coś nieoczekiwanego a Ty potrzebowałbyś pomocy, zaufana osoba będzie miała dostęp do twoich krytycznych kont.
3. Do logowania na kontach nie używaj publicznie dostępnych komputerów jakie można spotkać w hotelach oraz kawiarniach internetowych. Sprzęt w takich miejscach może być zarażony złośliwym oprogramowaniem przechwytującym sekwencję naciskanych klawiszy. Loguj się na swoje konta jedynie na zaufanych komputerach oraz urządzeniach mobilnych.
4. Uważaj na strony internetowe, które proszą o informacje dotyczące życia prywatnego. Takie pytania są zazwyczaj wykorzystywane w procedurze odzyskiwania hasła. Zagrożeniem mogą być odpowiedzi na pytania, które można znaleźć w internecie, lub na portalach społecznościowych takich jak Facebook. Upewnij się, że jeśli podajesz odpowiedzi na tego typu pytania, to używasz informacji, które nie są publicznie dostępne lub zmyślone. Programy do zarządzania hasłami, o których wspomnieliśmy wcześniej, mogą pomóc Ci w bezpiecznym przechowywaniu tego typu informacji.

Dobre hasła

5. Wiele z portali internetowych oferuje logowanie oparte o tzw. dwuskładnikowe uwierzytelnianie. Logując się w ten sposób, poza hasłem należy wprowadzić dodatkowy składnik np. kod wysłany na Twój telefon komórkowy. Opcja ta, jest znacznie bardziej bezpieczna niż używanie jedynie hasła. Jeśli portal, z którego korzystasz umożliwia włączenie takiej opcji, używaj jej.
6. Urządzenia mobilne w celu ochrony dostępu, często wymagają wprowadzenia kodu PIN. Pamiętaj, że jest on również formą hasła. Im dłuższy będzie Twój PIN, tym będzie on bezpieczniejszy. Wiele urządzeń umożliwia zmianę numeru PIN na wieloznakowe hasło lub odblokowanie urządzenia za pomocą danych biometrycznych, takich jak odcisk palca.
7. Jeśli nie używasz już danego konta, zamknij je, zablokuj lub usuń.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego.
Odwiedź securingthehuman.sans.org/ouch/archives i dowiedz się więcej.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Źródła

Menedżer haseł:	https://securingthehuman.sans.org/ouch/2015#october2015
Dwustopniowe uwierzytelnianie:	https://securingthehuman.sans.org/ouch/2015#september2015
Zablokuj swój login:	https://lockdownyourlogin.com
SANS SEC301 - Pięciodniowy kurs podstaw cyberbezpieczeństwa:	https://sans.org/sec301

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski