OUCH! | Lipiec 2015

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM WYDANIU..



# Media społecznościowe

## Wstęp

Portale społecznościowe takie jak Facebook, Twitter, Instagram oraz LinkedIn są wspaniałymi narzędziami pozwalającymi na utrzymywanie kontaktów z osobami z całego świata. Niestety, narzędzia te są na tyle potężne, że ich używanie niesie ze sobą ryzyko, nie tylko dla Ciebie jako bezpośredniego użytkownika, ale także dla Twojej rodziny, przyjaciół oraz pracodawcy. W tym wydaniu magazynu OUCH! wyjaśniamy te zagrożenia oraz omawiamy bezpieczny sposób ich używania.

### Redaktor gościnny

Tanya Baccam jest konsultantem bezpieczeństwa z wieloletnim stażem. Od ponad 10 lat jest autorką i instruktorką kursów Instytutu SANS takich jak SEC502, SEC542, SEC401, MGT414, AUD507 oraz wielu innych. Jest aktywna na Twitterze pod nickiem **@tbaccam**.

## Prywatność

Wspólnym problemem mediów społecznościowych jest ochrona informacji osobistych. Potencjalne zagrożenia mogące się pojawić przy nieodpowiednim użyciu portali społecznościowych to:

- **Wpływ na Twoją przyszłość**: niektóre firmy przeszukują portale społecznościowe jako część procesu rekrutacyjnego. Odnalezienie na nich nieodpowiednich wpisów lub zdjęć, nie ważne nawet jak starych, może spowodować, że nie otrzymamy angażu lub awansu. W dodatku wiele uniwersytetów także sprawdza profile kandydatów przed ich przyjęciem. Opcje prywatności na portalach społecznościowych nie zawsze mogą zadziałać, ponieważ instytucja może poprosić Cię o polubienie ich strony lub niektóre z postów mogą być zarchiwizowane na wielu różnych stronach internetowych i być nadal widoczne.
- **Ataki na Ciebie**: Twoje posty mogą być analizowane przez przestępców, którzy chcą uzyskać dostęp do danych Twoich lub Twojego pracodawcy. Na przykład mogą wykorzystać udostępniane przez Ciebie informacje do odgadnięcia odpowiedzi na pytania pomocnicze potrzebne do zmiany haseł, stworzyć spersonalizowany fałszywy email w celu przeprowadzenia ataku spear phishing (patrz OUCH! z lipca 2013), lub zadzwonić do Twojego pracodawcy i podszyć się pod Ciebie. W dodatku takie ataki mogą przenieść się do świata fizycznego, np. poprzez zidentyfikowanie Ciebie i odnalezienie miejsc, w których mieszkasz i pracujesz.
- **Przypadkowe szkody dla Twojego pracodawcy**: przestępcy lub konkurencja mogą wykorzystać wrażliwe informacje dotyczące Twojej firmy, które umieszczasz w Internecie, aby zaszkodzić Twojemu pracodawcy. Twoje posty mogą wyrządzić szkodę dla reputacji Twojej firmy. Zawsze sprawdź obowiązujące zasady odnośnie tego co możesz, a czego nie powinieneś udostępniać w sieciach społecznościowych nt. swojej pracy.

Najlepszym zabezpieczeniem jest ograniczenie tego co umieszczasz w sieci. To prawda, że ustawienia prywatności mogą pomóc w zapewnieniu, że Twoje posty są widoczne tylko dla wybranego grona osób, ale ustawienia z nimi związane często

# Media społecznościowe

się zmieniają i bywają niejednoznaczne. To co kiedyś było prywatne, może nagle stać się publiczne. Pamiętaj też, że prywatność Twoich wpisów jest zależna od tego z kim się nimi dzielisz. Im więcej osób może przeczytać Twój post, tym bardziej prawdopodobne, że stanie się on publiczny. Najlepiej będzie jeśli założysz, że cokolwiek co umieszczasz w sieci, prędzej czy później stanie się publicznie dostępne i niemożliwe do usunięcia.

Staraj się monitorować to, co Twoi znajomi umieszczają w Internecie na Twój temat. Jeśli jest to coś z czym czujesz się niekomfortowo, poproś aby taki wpis usunęli. Jeśli nie będą chcieli tego zrobić, skontaktuj się z administracją serwisu społecznościowego i poproś o usunięcie posta. Kieruj się takimi samymi pobudkami, gdy Ty umieszczasz w Internecie informacje na czyjś temat.



*Portale społecznościowe dają wiele zabawy, ale uważaj komu udostępniasz swoje informacje.*

## Bezpieczeństwo

Poza troską o zapewnienie prywatności informacjom jakie umieszczasz w sieci, kilka poniższych kroków pomoże Ci zapewnić bezpieczeństwo swoich kont w czasie używania serwisów online.

- **Login**: chroń każde ze swoich kont silnym, unikatowym hasłem (patrz OUCH! z maja i października 2013) i nie dziel się nim absolutnie z nikim. Warto pamiętać, że wiele z portali społecznościowych wspiera bezpieczniejsze formy uwierzytelnienia, jak np. dwustopniowe uwierzytelnienie. Zawsze używaj silnych metod uwierzytelnienia, kiedy to tylko możliwe.
- **Ustawienia prywatności**: jeśli stosujesz ustawienia prywatności, upewnij się, że regularnie je sprawdzasz. Portale społecznościowe często zmieniają ustawienia prywatności, co może prowadzić do pomyłek. Dodatkowo, wiele aplikacji umożliwia dodanie Twojej pozycji GPS do zamieszczanej na portalu treści. Jeśli nie chcesz, aby taka informacja była dodawana, zawsze sprawdzaj te ustawienia w danej aplikacji.
- **Szyfrowanie**: portale społecznościowe używają szyfrowania nazywanego HTTPS w celu zabezpieczenia połączeń do swoich serwerów. Niektóre ze stron takich jak Twitter lub Google+ używają go w standardzie, podczas gdy inne wymagają, aby włączyć tę metodę ręcznie. Sprawdź ustawienia swojego konta i włącz w nim obsługę szyfrowania jako opcję domyślną.
- **Email**: nie daj się nabrać na maile, które twierdzą, że pochodzą od administratorów serwisów społecznościowych - mogą to być próby podszycia się przez przestępców. Najbezpieczniejszą metodą na odpowiedź na taką wiadomość jest samodzielne zalogowanie się do serwisu społecznościowego, np. z zapisanej zakładki w przeglądarce, a następnie odesłanie odpowiedzi poprzez serwis.
- **Złośliwe linki i oszustwa**: uważaj na podejrzane linki i potencjalne oszustwa umieszczane na portalach społecznościowych. Przestępcy także korzystają z tych portali w celu dokonywania ataków. To, że daną wiadomość umieścił Twój znajomy, nie oznacza, że on jest jej autorem - jego konto mogło zostać przejęte. Jeśli ktoś z Twojej rodziny lub przyjaciół umieścił dziwną wiadomość, że np. zostali okradzeni i potrzebują wsparcia pieniężnego,

# Media społecznościowe

zadzwoń do takiego znajomego i upewnij się, że wiadomość jest prawdziwa.

- **Aplikacje mobilne**: większość z portali społecznościowych udostępnia aplikacje mobilne w celu umożliwienia dostępu do konta. Zawsze sprawdzaj, czy pobierasz aplikację z zaufanego miejsca. Upewnij się, że Twój smartfon jest zabezpieczony silnym hasłem, gdyż w przypadku zgubienia lub kradzieży mógłby zostać wykorzystany do uzyskania dostępu do Twoich kont i umieszczenia informacji w Twoim imieniu.

Portale społecznościowe to doskonałe narzędzia ułatwiające komunikację z całym światem. Przestrzegając naszych wskazówek, można cieszyć się wszystkimi ich możliwościami i jednocześnie pozostać bezpiecznym. Zapoznaj się z poradami na swoim portalu społecznościowym, aby dowiedzieć się w jaki sposób zgłaszać podejrzaną aktywność i pomóc w zapewnieniu bezpieczeństwa sobie jak i innym użytkownikom.

## 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 http://www.securingthehuman.org 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

## Przydatne linki

| | |
|---|---|
| Nowe oblicze hasła: | http://www.securingthehuman.org/ouch/2015#april2015 |
| Dwustopniowe uwierzytelnianie: | http://www.securingthehuman.org/ouch/2013#august2013 |
| Bezpieczne aplikacje mobilne: | http://www.securingthehuman.org/ouch/2015#january2015 |
| Naucz swoje dzieci cyberbezpieczeństwa: | http://www.securingthehuman.org/ouch/2015#june2015 |
| Facebook - Centrum Informacji o Bezpieczeństwie: | https://www.facebook.com/safety |



Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski