Bezpieczeństwo informatyczne użytkowników

kpt. Grzegorz Data
OISW w Rzeszowie

Rzeszów, maj 2018

Phishing

Phishing to jeden z najpopularniejszych ataków opartych o wiadomości e-mail, ale także coraz częściej o wiadomości na portalach społecznościowych. Przestępcy internetowi próbują Cię oszukać i spowodować, abyś podjął działanie zgodnie z ich zamierzeniami. Atakujący bardzo skrupulatnie przygotowują treść takich wiadomości. Mogą udać, że mail pochodzi od kogoś kogo znasz, jak na przykład od kolegi lub firmy, której ufasz. Potrafią nawet podrobić logo banku lub wysłać wiadomość z podobnego adresu. Cyberprzestępcy wysyłają takie wiadomości do tysięcy, a nawet milionów odbiorców na całym świecie.

Phishing

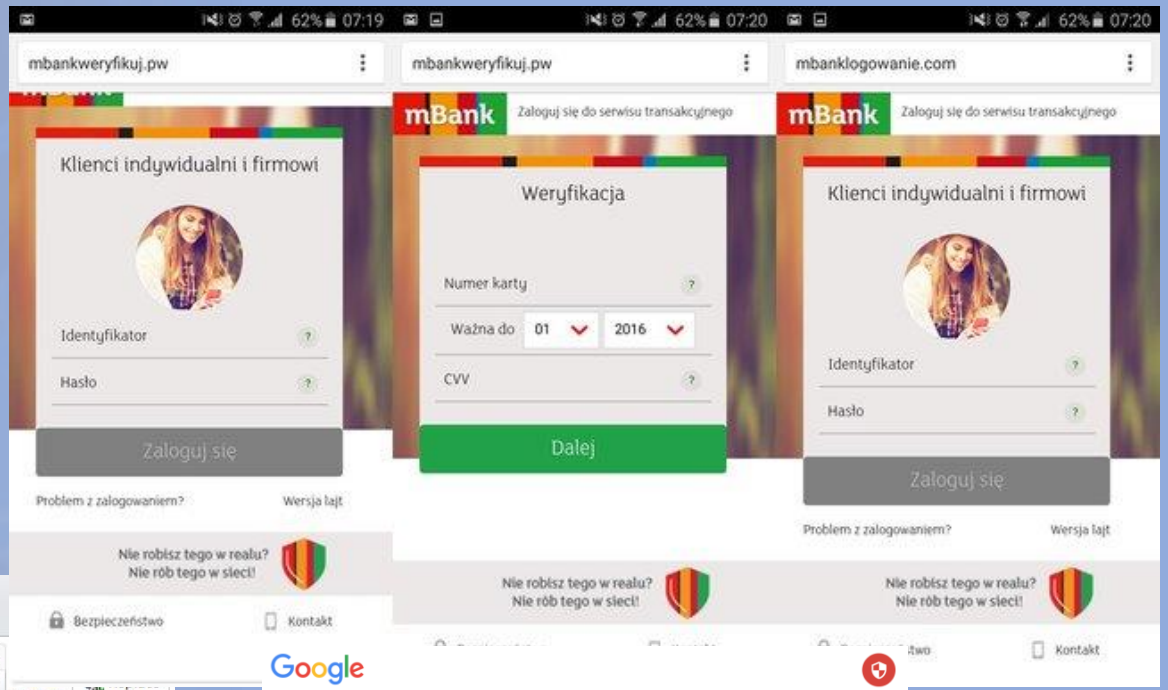
Celem atakującego jest zmanipulowanie Cię tak, abyś kliknął na link, który zabierze Cię na stronę pytającą o login i hasło, Twój ulubiony kolor czy nazwisko panieńskie matki. Takie strony bliźniaczo przypominają na przykład znane strony banku, jednak są zaprojektowane tylko po to, żeby wykraść dane potrzebne do uzyskania dostępu do Twojego konta bankowego czy numer karty kredytowej.

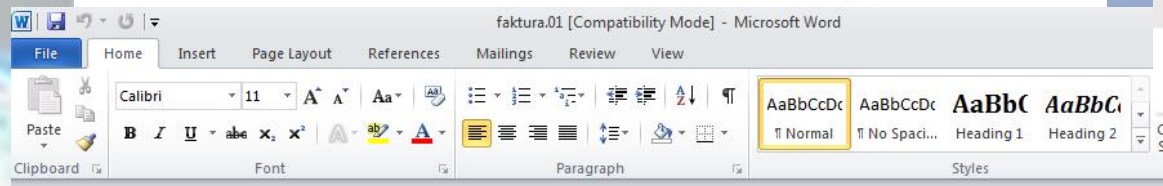
E-mail

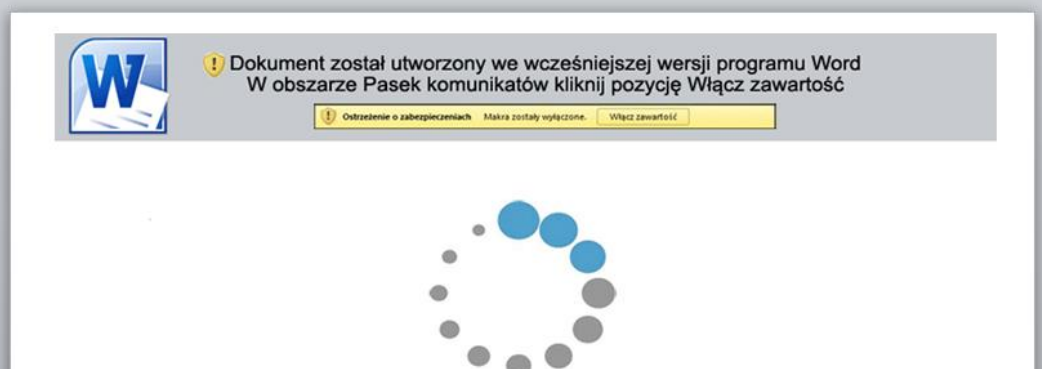
1. Czy znasz nadawcę wiadomości?
2. Czy otrzymywałeś już inne wiadomości od tego nadawcy?
3. Czy spodziewałeś się otrzymać tę wiadomość?
4. Czy tytuł wiadomości i nazwa załącznika mają sens?
5. Czy wiadomość nie zawiera podejrzanych załączników

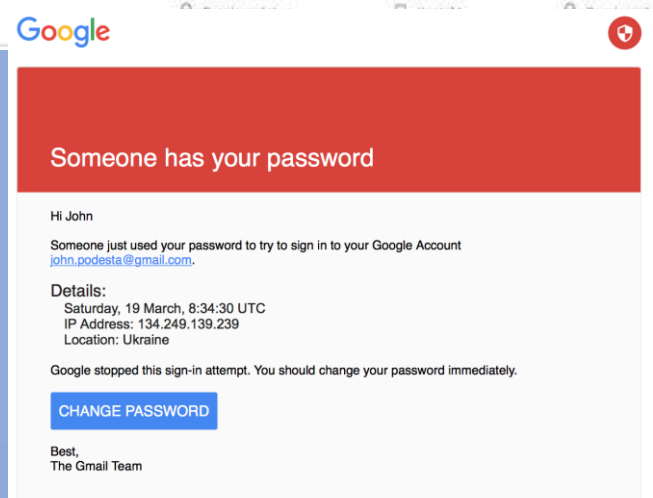
Użyj zdrowego rozsądku. jeśli treść wiadomości e-mail jest podejrzana lub zbyt obiecująca, najprawdopodobniej jest to atak

Przykłady phishingu









Inne przykłady

- Fałszywe rabaty i promocje
- Szkodliwe banery reklamowe
- Fałszywe wyniki wyszukiwania
- Fałszywe e-faktury
- Wiadomości o zablokowanym koncie
- Aukcje lub oferty (allegro, olx, itp.) – fałszywy link do płatności za np. przesyłkę - Dotpay PayU – atakujący może utworzyć zlecenie stałe – ostatnie przykłady tanie klocki lego, „oddam za darmo” na olx.

Porady

- Sprawdzaj linki (literówki), nie klikaj link do na witryny banku podaną w wiadomości.
- Wprowadzaj login i hasło tylko na stronach zabezpieczonych (https nie http)
- Prośby o ryzykowne zachowanie (przelew, pomoc finansowa) potwierdzaj telefonicznie – ktoś mógł przejąć konto pocztowe, Facebook, uzyskać możliwość wysłania SMS.
- Często wiadomości wyłudzające informacje są tłumaczone automatycznie – zwracaj uwagę na błędy literowe, brak znaków diakrytycznych, niestaranny wystój graficzny witryny.
- Staraj nie logować się do banku z ogólnodostępnych sieci Wi-Fi
- Zgłaszaj podejrzane maile informatykom

Sieci społecznościowe

- Nie jesteśmy klientem – jesteśmy PRODUKTEM
  facebook dziennie – 2,2 mld użytkowników, 1,45 loguje się codziennie, 10 mln razy dziennie ktoś daje LikeIt lub udostępnia, 300mln zdjęć – FACEBOOK NIE TWORZY ŻADNEJ TRESCI
- Firmy sprzedają możliwość reklamowania firmom swoich produktów nam na podstawie treści naszych maili, naszych preferencji, zawartości kalendarza, treści SMS, naszych rozmów głosowych, zapytań w wyszukiwarce, położenia geograficznego. (Google, Facebook, Twitter, LinkedIn, Instagram)
- Co trzeci wniosek rozwodowy w USA i Wielkiej Brytanii zawiera jako jedną z przyczyn Facebook
- 86,1 komend policji w USA przeszukuje sieci społecznościowe w ramach prowadzonych śledztw

Sieci społecznościowe

- Według regulaminu Google:

Przesyłając materiały w jakikolwiek sposób do Usług, użytkownik udziela firmie Google (i jej współpracownikom) ważnej na całym świecie licencji na wykorzystywanie, udostępnianie, przechowywanie, reprodukowanie, modyfikowanie, przesyłanie, publikowanie, publiczne prezentowanie i wyświetlanie oraz rozpowszechnianie tych materiałów, a także na tworzenie na ich podstawie dzieł pochodnych (na przykład przez wykonanie tłumaczenia, adaptacji lub innych zmian)

Targetowanie

targeting behawioralny”, „targeting predyktywny” albo „analiza behawioralnych cech osobistych”: chodzi o jak najdokładniejsze opisanie nas, żeby informacje gromadzone przez brokerów można było sprzedać za jak najwyższą ceną agencjom reklamowym i marketingowym oraz innym firmom, które potrzebują ich do podejmowania decyzji biznesowych – pieluchy lepiej się sprzedaje ciężarnej 30 letniej gospodyni domowej niż 19 letniemu studentowi.

Targetowanie

Przykłady:

- Ojciec 15 letniej córki dowiedział się ze zostanie dziadkiem od firmy Target przysyłającej kupony rabatowe. Po awanturze „Moja córka dostała to pocztą! (...) Ona jest jeszcze w liceum, a wy przysyłacie jej kupony na ubranka dziecięce i łóżeczka? Chcecie ją zachęcić do zajścia w ciążę?” przeprosił – okazało się ze to prawda. Target zastosował „algorytm ciąży” – analizując zachowanie klientów – wynikło, iż kobiety mogące być w ciąży „kupują na początku drugiego trymestru więcej bezzapachowego balsamu do ciała oraz suplementów diety zawierających wapń, magnez i cynk” – 25 produktów kupowanych w mniejszej lub większej grupie wskazywały na „możliwość bycia w ciąży” dzięki temu można było dotrzeć do milionów nowych klientek.

Viktor Mayer-Schönberger, Kenneth Cukier, „*Big Data: A Revolution That Will Transform How We Live, Work, and Think*”, Houghton Mifflin Harcourt, Boston 2013, s. 58.

Targetowanie

Przykład Cambridge Analitica: algorytm stworzony przez dr Michała Kosińskiego na podstawie wystawionych „lajków” i udostępnionych postów ma zbudować profil psychologiczny człowieka. Algorytm zastosowano do tworzenia spersonalizowanych reklam przy wyborach w USA.

Wg twórców algorytm był w stanie ocenić osobowość badanego człowieka z większą dokładnością, niż zrobił to kolega z pracy, na podstawie zaledwie 10 polubień. Po przeanalizowaniu 70 lajków komputer był bardziej trafny w ocenie niż przyjaciele i współlokatorzy, a rodziców i rodzeństwo pokonywał przy 150 lajkach. Najtrudniej było prześcignąć współmałżonka, ale i to się udawało przy 300 polubieniach

Źródło https://applymagicsauce.com/.

Targetowanie

„Jeżeli robisz coś, o czym według ciebie nikt nie powinien się dowiedzieć, być może w pierwszej kolejności należałoby przestać”

Erik Schmidt dyr. Gen. Google na pytanie o intensywne śledzenie użytkowników

„*prywatność przestała być normą społeczną*”

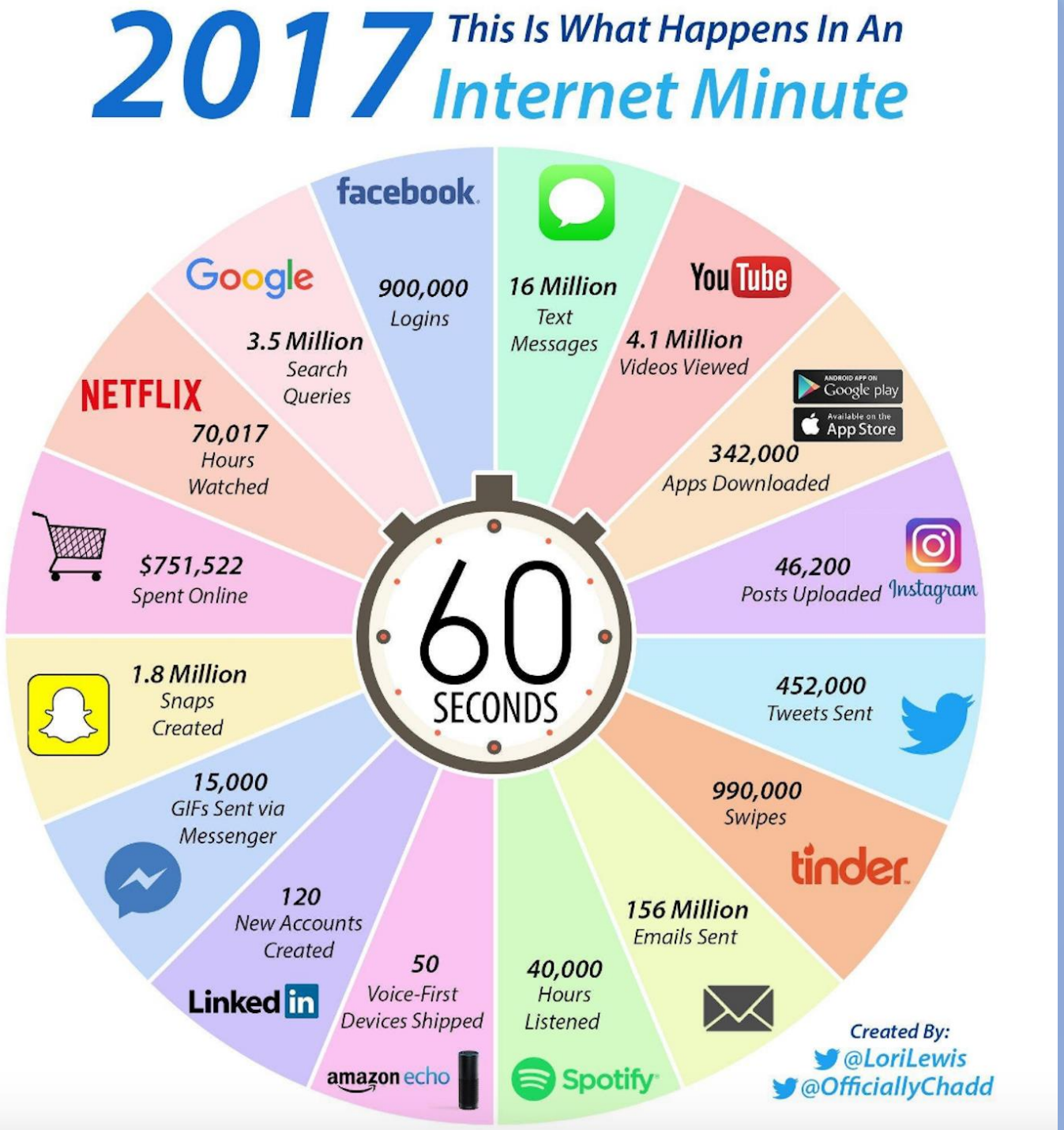
właściciel facebook’aMark Zuckerberg

Co wie o mnie Google

- https://www.google.com/ads/preferences/
- https://maps.google.com/locationhistory
- https://history.google.com
- https://security.google.com/settings/security/activity
- https://security.google.com/settings/security/permissions
- https://www.google.com/takeout

Co wie o mnie Facebook

- Należy kliknąć na ikonkę trójkąta skierowanego w dół, Wejść w Ustawienia. W zakładce Prywatność jest także dostępna opcja „Przejrzyj wszystkie swoje posty i rzeczy, w których Cię oznaczono". Dodatkowo, w Dzienniku aktywności można sprawdzić swoją historię wyszukiwania, przejrzeć treść prowadzonych konwersacji czy zobaczyć swoje komentarze.
- Dodatkowo: przewiń w dół ogólne ustawienia konta i kliknij „Pobierz kopię swoich danych z Facebooka”, wpisz swój adres e-mail. Gdy dane będą gotowe, zostaniesz poproszony o ponowne wprowadzenie hasła.
- Dzięki temu dowiesz się, jakie posty, filmy i zdjęcia udostępniłeś od założenia konta. Dodatkowo, jakie rozmowy prowadziłeś na czacie. W spisie pojawi się także wiele innych ciekawych informacji – Adresy IP, zameldowania, numery telefonów, rozpoznane twarze. Jeśli pozwoliłeś Messengerowi obsługiwać SMSy ich treść także będzie dostępna.



Innymi słowy w kilka minut generujemy tyle informacji co poprzednie 10 tysięcy pokoleń razem wzięte

6 terabajtowy dysk kosztuje około 500 PLN, a może pomieścić całą muzykę nagraną dotychczas na świecie

McKinsey Global Institute, *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, maj 2011; Kevin Kelly, przemówienie podczas konferencji Web 2.0 w 2011 roku, https://www.youtube.com/watch?v=kPso8i7Mv00

Opinie, marketing szeptany

- Prawie 90% osób przyznaje, że opinie znalezione w Internecie mają wpływ na ich decyzje zakupowe, a firma Nielsen ustaliła ponadto, że zaskakująco dużo, bo aż 70% ludzi ufa opiniom znalezionym w sieci tak jak rekomendacjom przyjaciół
- Pond 25% opinii jest fałszywe – cena od 1 do 3 zł / szt.

.

Hasła

Hasła są jak bielizna:

- Zmieniaj regularnie
- Noś tak by inni nie widzieli, nie pozostawiaj na widoku
- Nie pożyczaj innym

- Z rozwagą korzystaj z sieci bezprzewodowych
- Nie używaj znalezionych pendrive’ów oraz kart SD
- Rób kopie zapasowe danych
- Aktualizuj oprogramowanie na komputerach oraz urządzeniach.
- Nie zamieszczaj w Intrernecie informacji kiedy i gdzie wyjeżdżasz – to zaproszenie dla złodzieja.

Telefony

- W razie zagubienia :
  ANDROID: Wejdź na android.com/find i zaloguj się na konto Google – możesz odnaleźć położenie swojego telefonu, odtworzyć dźwięk, zablokować lub wykasować na nim dane;
  APPLE: Zaloguj się na stronie icloud.com/find na komputerze. Będziesz mógł zobaczyć położenie telefonu na mapie a także zablokować go kodem PIN włączając tryb „Utracony”;
  MICROSOFT: Przejdź na stronę account.microsoft.com/devices. Jeśli zostanie wyświetlony monit o zalogowanie się, użyj tego samego konta Microsoft, które zostało użyte do zalogowania się na telefonie. Wybierz telefon, który chcesz znaleźć, a następnie kliknij pozycję Znajdź mój telefon. Istnieje także możliwość zadzwonienia na telefon bądź zablokowania hasłem a także wymazania;
- Instaluj aplikacje z zaufanych źródeł, sklepu Gogle Play lub oficjalnego sklepu Apple, instalując zweryfikuj ustawienia prywatności, o które będzie pytać podczas instalacji – czy np. aplikacja musi mieć dostęp do listy Twoich znajomych z informacjami kontaktowymi;
- Przy sprzedaży lub oddaniu telefonu usuń wszystkie dane poprzez opcje:
  APPLE : Ustawienia/Ogólne/Wyzeruj/Wymaż zawartość i ustawienia
  ANDROID: Ustawienia/Kopie i kasowanie danych/Ustawienia Fabryczne

Cyberwojna?

- https://botnet-cd.trendmicro.com/
- https://www.fireeye.com/cyber-map/threat-map.html
- http://map.norsecorp.com/
- https://cybermap.kaspersky.com/
- https://threatmap.checkpoint.com/ThreatPortal/livemap.html
- https://threatmap.fortiguard.com/
- http://www.digitalattackmap.com/

Dziękuję za uwagę

kpt. Grzegorz Data

OISW w Rzeszowie

tel: 17 8580775

voip: 6021060

email: grzegorz.data@sw.gov.pl

JID: 021036gdat@swnet.sw.gov.pl