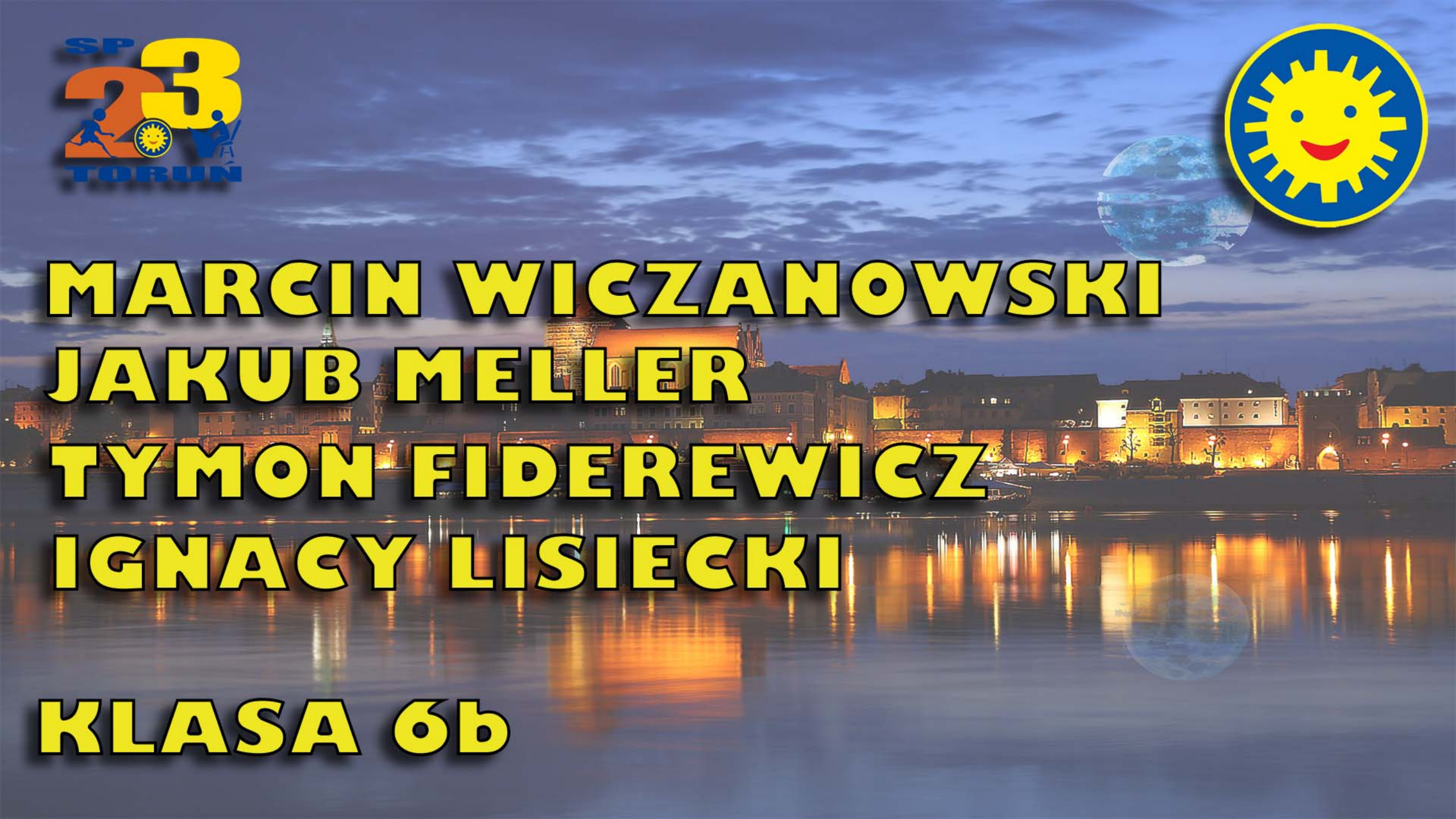

SP
23
TORUŃ
MARCIN WICZANOWSKI
JAKUB MELLER
TYMON FIDEREWICZ
IGNACY LISIECKI
KLASA 6b

PHISHING I JEGO PRZYKŁADY

TECHNIKI STOSOWANE PODCZAS ATAKÓW CYBERNETYCZNYCH

- SOCJOTECHNIKI
- ZŁOŚLIWE OPROGRAMOWANIE
- KRADZIEŻ TOŻSAMOŚCI
- BLOKOWANIE DOSTEPU DO USŁUG I ZASOBÓW

RODZAJE ATAKÓW CYBERNETYCZNYCH

Ataki techniczne

Czyli takie, które wymagają określonego poziomu wiedzy informatycznej oraz znajomości odpowiednich narzędzi technicznych. Zazwyczaj atakują zasoby i infrastrukturę teleinformatyczną ofiary.

Ataki socjotechniczne

Czyli takie, których celem są ludzie. Według definicji SANS.org atak socjotechniczny „jest rodzajem ataku psychologicznego polegającym na tym, że atakujący nakłania swoją ofiarę do wykonania jakiejś czynności”.
Atak taki jest potocznie nazywany z angielskiego **SCAM-em.**

CO TO JEST PHISHING

1

Rozsyłanie wiadomości elektronicznych przez oszustów podszywających się pod organizacje społeczne, banki czy różnego rodzaju zaufane instytucje.
Celem cyberprzestępców jest nakłonienie ofiary do pobrania złośliwego oprogramowania zawartego w załączniku maila bądź otworzenia podejrzanego odnośnika.
Wirusy i fałszywe strony internetowe nierzadko wykradają poufne informacje, dane logowania, a nawet numery kart płatniczych.
Maile phishingowe są skierowane do setek lub tysięcy użytkowników.

2

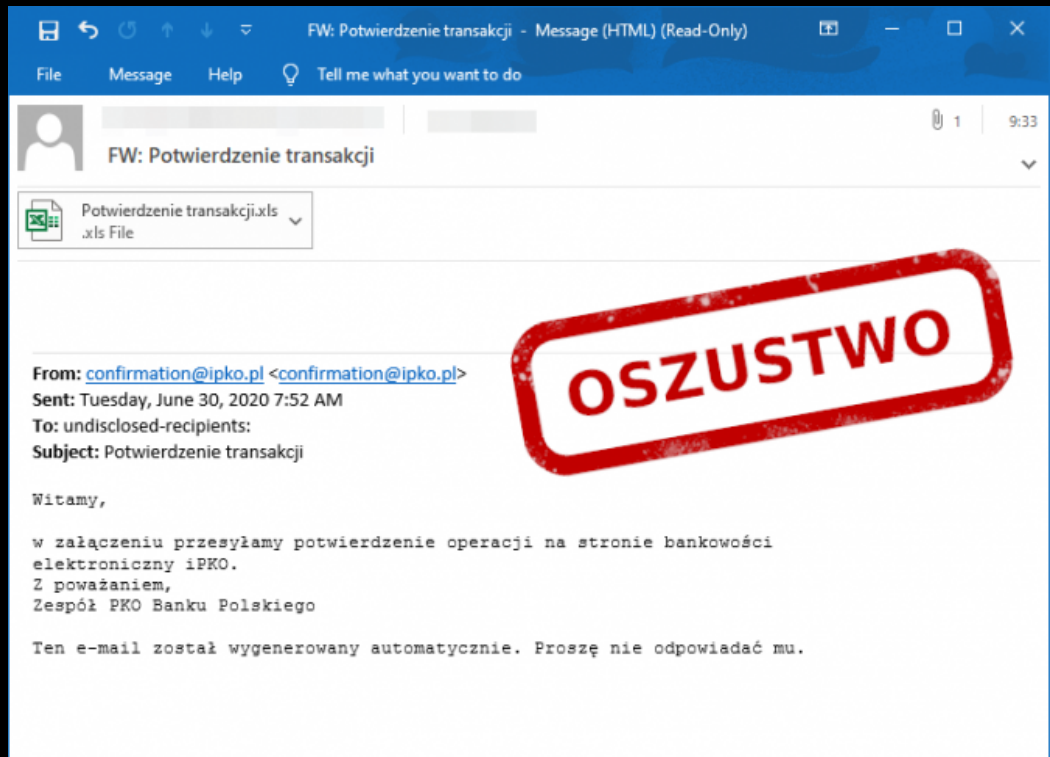
Phishing to metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań.

3

Phishing - wyłudzanie informacji umożliwiających nielegalny dostęp do cudzych zasobów, przeważnie elektronicznych rachunków bankowych karty kredytowej lub nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.

PHISING E-MAIL

Najpopularniejszym rodzajem phishingu jest ten mailowy. Z pewnością Twoja skrzynka (a szczególnie folder SPAM) pełna jest tego typu dziwnych wiadomości wysyłanych masowo — od informacji o zablokowanym koncie w jakimś serwisie po rzekome faktury do pilnego opłacenia.



ELEMENTY E-MAILI PHISHINGOWYCH

ZAŁĄCZNIKI

Fałszywe faktury, potwierdzenia zamówieńc zy zaproszenia na wydarzenia.
Otwarcie phishingowego załącznika może skutkować na przykład pobraniem na urządzenie złośliwego oprogramowania, którego celem jest wykradanie poufnych danych.
Jak się chronić? Osobiście skontaktuj się z n adawcą, dzwoniąc lub wysyłając nową wiadomość e-mail, ale nie używając opcji odpowiedz” .

ODNOŚNIKI

Linki do specjalnie utworzonych witryn internetowych, które imitują inne, godne zaufania i popularne strony.
Oszuści wysyłają hurtowe wiadomości z linkami do złośliwych witryn, prosząc odbiorców o zalogowanie się do profilu al bo potwierdzenie danych osobowych.
Fałszywe strony internetowe najczęściej wykradają podane dane albo zawierają złośliwe oprogramowanie.
Najedź kursorem na link i sprawdź, czy w ygląda normalnie.
Podrobione odnośniki mogą zawierać literówki (np. Netflx zamiast Netflix) albo nie mieć przedrostka „https”.

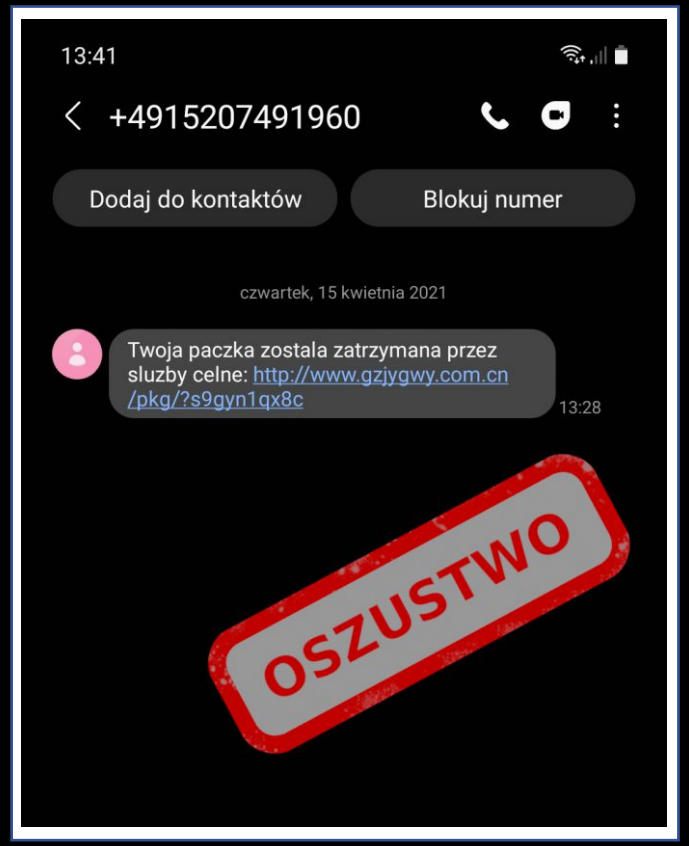
FAŁSZYWI NADAWCY

Ustawienie nazwy nadawcy w opcjach poczty elektronicznej - najedź kursorem na pole „Nadawca”, by podejrzeć adres mailowy wysyłającego wiadomość.
Końcówki: gmail.com czy o2.pl najpewniej należą do osób prywatnych.

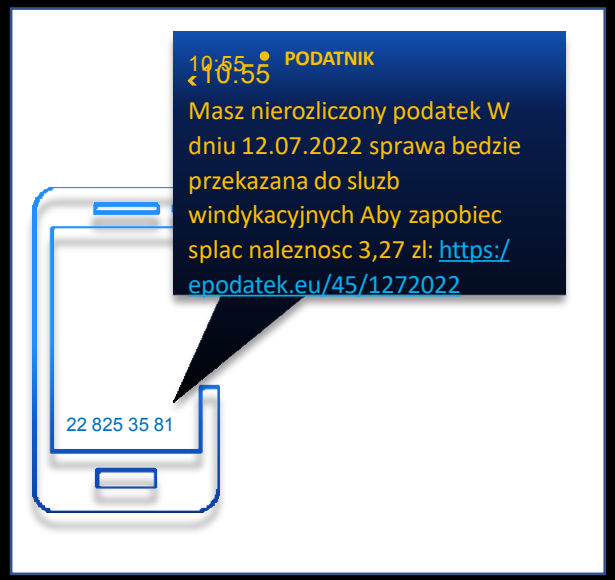
SMS PHISHING (SMISHING)

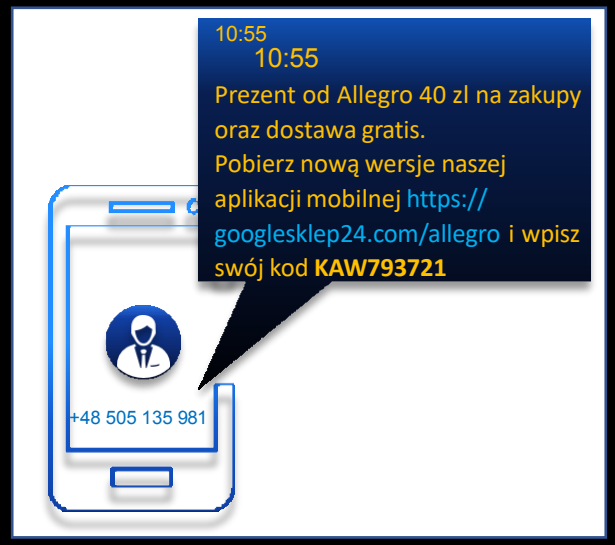
Phishing przez wiadomości SMS nazywany jest smishingiem.
W dobie zalewu spamu i coraz lepszych filtrów antyspamowych w skrzynkach e-mail, część phisherów przerzuciła się na wysyłkę wiadomości SMS — te w przeciwieństwie do e-maili odczytuje praktycznie każdy.
A dodatkowo w prosty sposób można wysyłać wiadomości z dowolną nazwą nadawcy SMS-a.
Może to być np. popularny SMS z dopłatą brakującej niewielkiej kwoty za fakturę operatora prądu, gazu, wody, internetu

Przykład Smishingu:



ATAK PHISHINGOWY – SMS PRZYKŁADY





PHISHING TELEFONICZNY (VISHING)

Mniej popularnym rodzajem phishingu jest phishing przez telefon
(czyli: Vishing).
Atak ten wymaga trochę więcej zachodu ze strony przestępców, bo w końcu po drugiej stronie słuchawki musi być żywy człowiek, który do Ciebie dzwoni.
Niestety skuteczność takich ataków jest duża. Tym bardziej że tak jak w poprzednim przypadku, tak i tutaj phisherzy mogą dzwonić z dowolnie wybranego przez siebie numeru (np. numeru infolinii banku), który wyświetli się na twoim telefonie.

Przykład Vishingu:

Przykład takiego ataku (phishing bankowy) w formie telefonu od fałszywego pracownika banku.

PHISHING WYSZUKIWARKOWY

Phishing wyszukiwarkowy, znany też jako zatrucie SEO lub trojan SEO, to działania hakerów nakierowane na zdobycie wysokiej pozycji w wynikach wyszukiwania wyszukiwarki internetowej.
Kiedy użytkownik kliknie taki odnośnik, zostanie przeniesiony na spreparowaną stronę internetową.
Za jej pomocą przestępcy mogą zebrać dane związane z interakcją lub skłonić go do podania wrażliwych informacji.
Hakerzy mogą podszywać się pod każdą stronę internetową, ale najczęściej wybierają strony banków, usług transferu pieniędzy, mediów społecznościowych i sklepów internetowych.

SPEAR PHISHING

Wymyślony scenariusz jest wykorzystywany do zwabienia potencjalnej ofiary, aby zwiększyć prawdopodobieństwo, że da się nabrać i uwierzy w historię. Jest to fałszywy motyw, zazwyczaj obejmujący jakąś rzeczywistą wiedzę o ofierze (np. datę urodzenia, numer PESEL itp.), mający na celu uzyskanie jeszcze większej ilości informacji.

Aby był maksymalnie skuteczny, atakujący musi wcześniej dobrze rozeznać swój cel - gdzie pracuje, z jakimi osobami utrzymuje kontakty, jakimi rzeczami zajmuje się w swojej pracy.
Każda informacja (w tym pozyskanie wcześniej firmowych dokumentów, w wyniku ataku na inne osoby z tej samej organizacji) zwiększa szansę na uwiarygodnienie się sprawcy i sukces jego działań.

Fałszywa korespondencja, która trafi do ofiary spear phishingu, będzie adresowana przeważnie jej imieniem, funkcją i nazwiskiem. Mail taki będzie pochodził pozornie od osoby, która zna cel działań, bądź organizację, z którą współpracuje. Mail będzie spersonalizowany i całkiem możliwe, że poświęcony sprawie, którą ofiara naprawdę się zajmuje.

Social Engineer tworzy adres e-mail, który wygląda jak napisany przez kierownictwo. Może być wysłany z fałszywej domeny podobnej do firmowej.
Na przykład: anowak@mon.gov.pl - fałszywa domena, która wygląda jak prawdziwa (dodano jedną literę pisaną czcionką w rozmiarze 0) przyciągnie uwagę, z właszcza jeśli podane będzie właściwe nazwisko wysyłającego.

DZIĘKUJĘ ZA UWAGĘ

Marcin WICZANOWSKI, Ignacy Lisiecki,
Tymon Fiderewicz, Jakub Meller
SP 23 Klasa 6b

Źródło zdjęć:
Internet licencja Creative Commons