Penetration Testing Professional

SOCIAL ENGINEERING

Section 2: Network Security – Module 8

v5.0

8. Social Engineering

- 8.1 What is it?
- 8.2 Types of Social Engineering
- 8.3 Samples of Social Engineering Attacks
- 8.4 Pretexting Samples
- 8.5 Tools

WHAT IS IT?

8.1. What is it?

Perfected by John Draper (Cap'n Crunch) in the days of Phreaking (Phone Hacking) and used by Kevin Mitnick to gain access to many company systems, Social Engineering is one of the oldest hacking techniques around.

8.1. What is it?

The premise behind social engineering is to exploit the human factor. In other words, putting people in situations where they will rely on the most common forms of social interactions:

- The desire to *be helpful*
- The tendency to *trust people*
- The *fear* of getting in *trouble*
- *Conflict avoidance*

8.1. What is it?

By preying on the human factor of system access, many times hackers do not have to navigate around the system security of an organization.

The hackers just engages employees inside the company to do that for them.

8.1. What is it?

Instead of spending countless hours trying to infiltrate systems, dump password hashes, crack them and so on, often times a simple “real world” support scenario can either yield all needed information or, install malware inside the company in a matter of minutes.

8.1. What is it?

More recently, the advent of *Social Networking* has vastly improved the ability of social engineers. As a result, both their ability to trick people into providing sensitive information and lead people into their social engineering exploits has improved.

One of the many ways this can be done, is by sending quizzes or surveys on social networks like Facebook.

8.1. What is it?

The “update this” and forward on forms, can actually divulge a great deal of information about someone. People are readily filling them out and posting them on their profiles:

- When was the last time you took a moment to review the actual information available on the web about you?
- Have you sent any opt-out requests to have information about you removed from a website?
- Were you even aware that you could do this?

8.1. What is it?

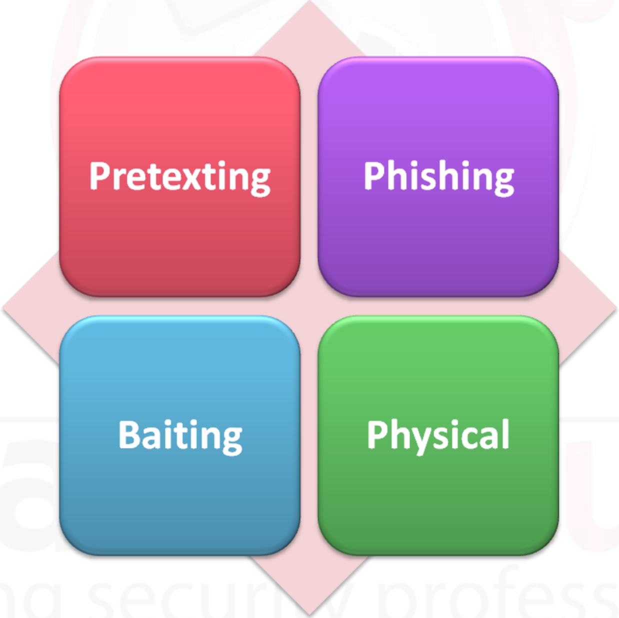
While Social Engineering was often a viable attack path for hackers, it was often overlooked by penetration testers until recently.

Having a social engineering aspect to pen-testing is a vital service to your company or clients to show them weaknesses within their employee education.

Types of Social Engineering

8.2. Types of Social Engineering

Let us take a look at some common forms of social engineering.



Pretexting

Pretexting is the art of placing a person in a realistic but fake situation, in order to get them to divulge information such as social security, bank account, user id and passwords.

An example of such an invented scenario may be to impersonate a help desk employee and assisting another target employee with either a data move or software update.

8.2.1. Pretexting

In a similar situation, the help desk technician may have the employee download an update for their machine, thereby tricking the employee into running malware on their system.

Pretexting often involves a great deal of research and planning in order to be able to specifically target employees within an organization. Persistence is often the key, as eventually there will be someone either more than willing to divulge the necessary information or, perform the necessary action(s) in order to be a helpful employee.

Phishing

Unlike Pretexting, Phishing is an attack that utilizes a fraudulent email, in order to coerce people into executing malicious code or revealing pertinent information.

- The email is crafted in a way to make it appear as if it is from a legitimate company.
- In addition, this can be a really cool advertisement for a product that no one would want to live without.

8.2.2. Phishing

There are types of phishing attacks which target a specific group of individuals for the purpose of obtaining specific type of information. Some type of phishing schemes are:

Whaling

Targets Executives in an organization, such as the CFO for gaining specific types of information.

Spear Phishing

Targets specific individuals within an organization, to try and circumvent detection.

Baiting

Baiting takes advantage of one of the most basic traits of humanity, “Curiosity”.

In baiting, a social engineer will leave media such as a CD, DVD or USB Stick in a conspicuous location, relying on the curiosity factor of a passerby to pick up the media and attempt to “take a look” at its contents.

8.2.3. Baiting

The engineer will place malware such as keystroke loggers, backdoors, etc. on the media, in order to either gain access or gather information from any system that tries to read the media.

8.2.4. Physical

Physical

Social Engineering can also take on a more physical form. In this case, the engineer will try and gain access to a facility or a restricted area. This is often accomplished by either *piggybacking* or *shadowing* a person into an entrance.

The pen test engineer may wear a fake badge in order to both trick the person they are following and, if they loose the person they followed in, be more convincing to other staff.

8.2.4. Physical

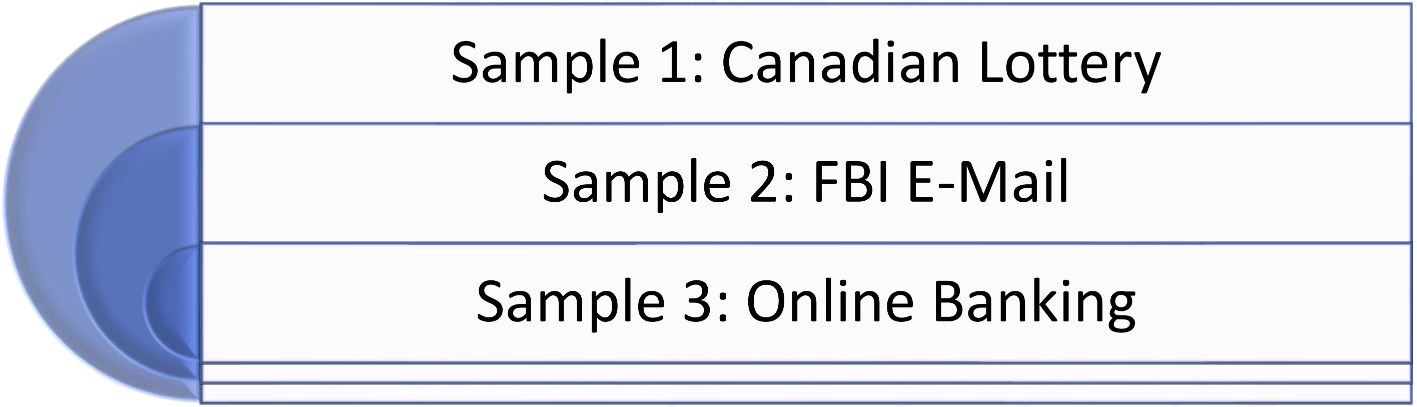
Most organizations lack proper training for their staff when it comes to simple observation as to the validity of an ID badge.

Many times, employees are wary of confrontation therefore, they either avoid asking someone to see the ID badge or, challenge the person following them in.

Samples of Social Engineering Attacks

8.3. Samples of Social Engineering Attacks

Let us first take a look at some common types of spam messages. These are examples right out of the spam folder in one of our email accounts.



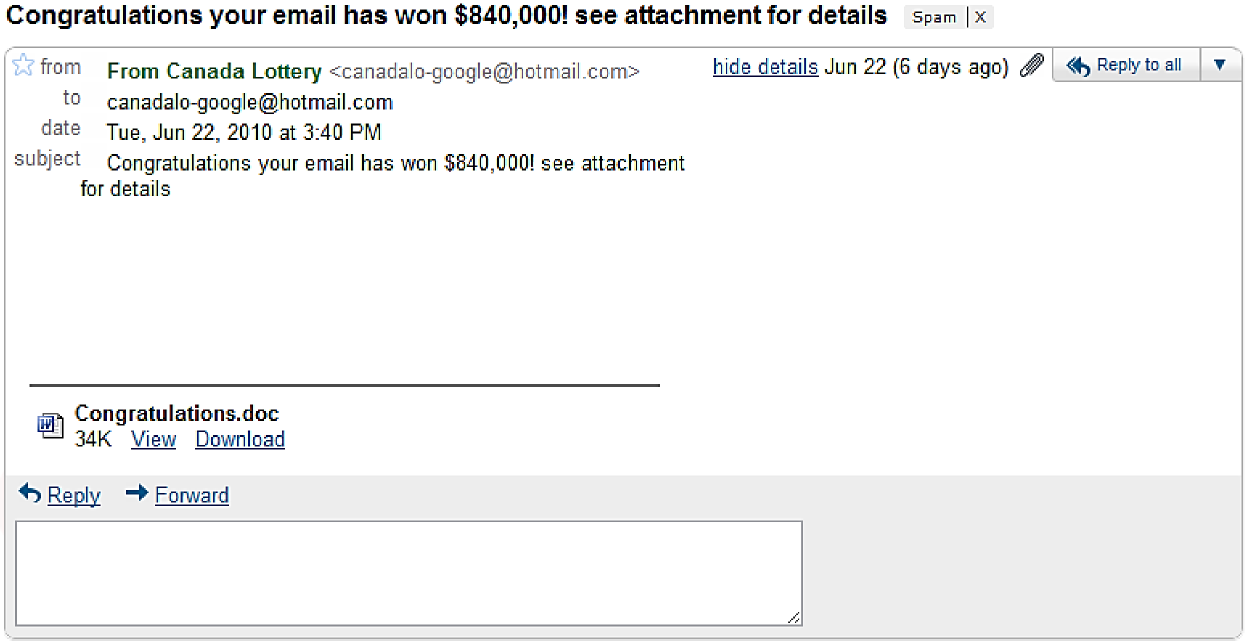
Sample 1: Canadian Lottery

Sample 2: FBI E-Mail

Sample 3: Online Banking

8.3.1. Sample 1: Canadian Lottery

The first example is a common scam which advertises that the recipient is the winner of the Canadian Lottery.



Congratulations your email has won $840,000! see attachment for details

from **From Canada Lottery** <canadalo-google@hotmail.com>

to canadalo-google@hotmail.com

date Tue, Jun 22, 2010 at 3:40 PM

subject Congratulations your email has won $840,000! see attachment for details

Congratulations.doc
34K View Download

8.3.1. Sample 1: Canadian Lottery

It appears we have won $840,000, but we need to open the attachment to see the details.

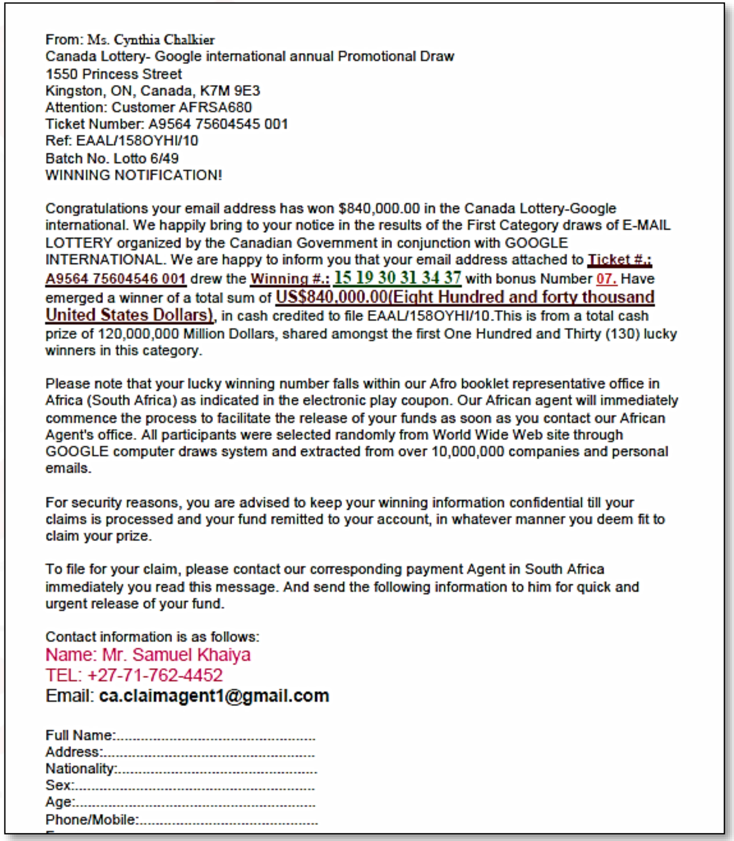
Before opening this attachment, we download and scan it with our local Anti-Virus solution.

The scan comes up clean, but we always prefer to be doubly safe, so we also submit it to Virus Total for a further review.

http://www.virustotal.com/

8.3.1. Sample 1: Canadian Lottery

Once we know it is clear, we can go ahead and open the attachment, which looks like this:



From: Ms. Cynthia Chalkier
Canada Lottery- Google international annual Promotional Draw
1550 Princess Street
Kingston, ON, Canada, K7M 9E3
Attention: Customer AFRSA680
Ticket Number: A9564 75604545 001
Ref: EAAL/158OYHI/10
Batch No. Lotto 6/49
WINNING NOTIFICATION!

Congratulations your email address has won $840,000.00 in the Canada Lottery-Google international. We happily bring to your notice in the results of the First Category draws of E-MAIL LOTTERY organized by the Canadian Government in conjunction with GOOGLE INTERNATIONAL. We are happy to inform you that your email address attached to Ticket #.: A9564 75604546 001 drew the Winning #.: 15 19 30 31 34 37 with bonus Number 07. Have emerged a winner of a total sum of **US$840,000.00(Eight Hundred and forty thousand United States Dollars)**, in cash credited to file EAAL/158OYHI/10.This is from a total cash prize of 120,000,000 Million Dollars, shared amongst the first One Hundred and Thirty (130) lucky winners in this category.

Please note that your lucky winning number falls within our Afro booklet representative office in Africa (South Africa) as indicated in the electronic play coupon. Our African agent will immediately commence the process to facilitate the release of your funds as soon as you contact our African Agent's office. All participants were selected randomly from World Wide Web site through GOOGLE computer draws system and extracted from over 10,000,000 companies and personal emails.

For security reasons, you are advised to keep your winning information confidential till your claims is processed and your fund remitted to your account, in whatever manner you deem fit to claim your prize.

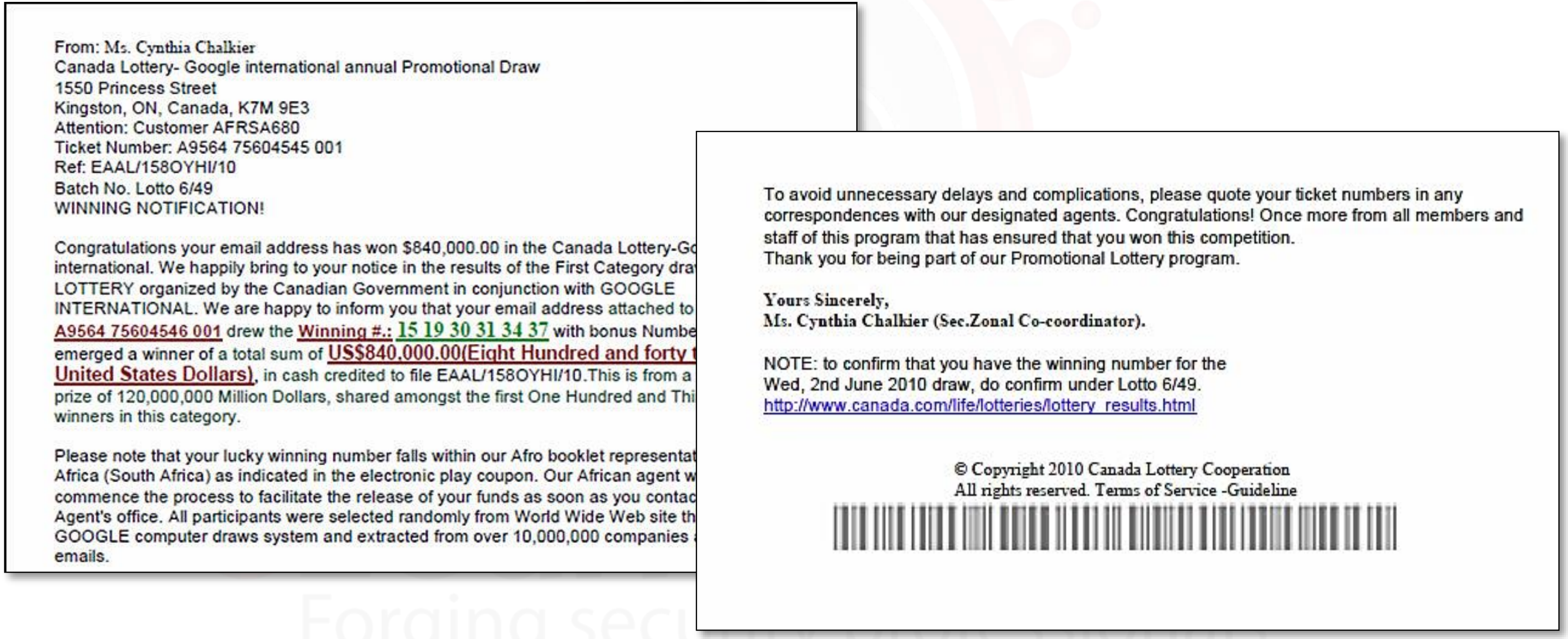
To file for your claim, please contact our corresponding payment Agent in South Africa immediately you read this message. And send the following information to him for quick and urgent release of your fund.

Contact information is as follows:
Name: Mr. Samuel Khaiya
TEL: +27-71-762-4452
Email: **ca.claimagent1@gmail.com**

Full Name:..
Address:...
Nationality:..
Sex:...
Age:...
Phone/Mobile:..

8.3.1. Sample 1: Canadian Lottery

Here are few others screenshots of the attachment:



From: Ms. Cynthia Chalkier
Canada Lottery- Google international annual Promotional Draw
1550 Princess Street
Kingston, ON, Canada, K7M 9E3
Attention: Customer AFRSA680
Ticket Number: A9564 75604545 001
Ref: EAAL/158OYHI/10
Batch No. Lotto 6/49
WINNING NOTIFICATION!

Congratulations your email address has won $840,000.00 in the Canada Lottery-Go
international. We happily bring to your notice in the results of the First Category dra
LOTTERY organized by the Canadian Government in conjunction with GOOGLE
INTERNATIONAL. We are happy to inform you that your email address attached to
A9564 75604546 001 drew the Winning #.: 15 19 30 31 34 37 with bonus Numbe
emerged a winner of a total sum of US$840,000.00(Eight Hundred and forty t
United States Dollars), in cash credited to file EAAL/158OYHI/10.This is from a
prize of 120,000,000 Million Dollars, shared amongst the first One Hundred and Thi
winners in this category.

Please note that your lucky winning number falls within our Afro booklet representat
Africa (South Africa) as indicated in the electronic play coupon. Our African agent w
commence the process to facilitate the release of your funds as soon as you contac
Agent's office. All participants were selected randomly from World Wide Web site th
GOOGLE computer draws system and extracted from over 10,000,000 companies
emails.

To avoid unnecessary delays and complications, please quote your ticket numbers in any correspondences with our designated agents. Congratulations! Once more from all members and staff of this program that has ensured that you won this competition.
Thank you for being part of our Promotional Lottery program.

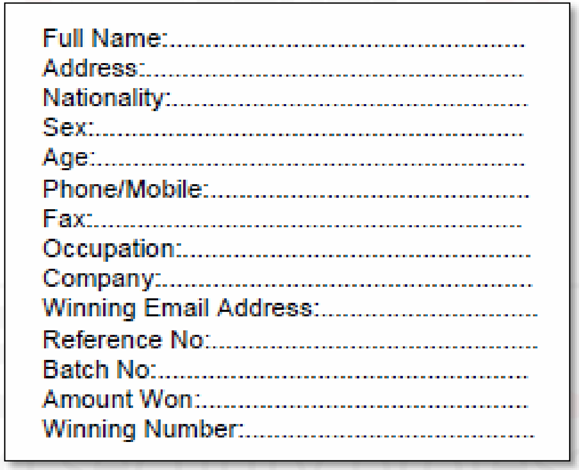
Yours Sincerely,
Ms. Cynthia Chalkier (Sec.Zonal Co-coordinator).

NOTE: to confirm that you have the winning number for the
Wed, 2nd June 2010 draw, do confirm under Lotto 6/49.
http://www.canada.com/life/lotteries/lottery_results.html

© Copyright 2010 Canada Lottery Cooperation
All rights reserved. Terms of Service -Guideline

8.3.1. Sample 1: Canadian Lottery

As we dissect the attachment, we see we are in possession of the wining number and to claim our money we email the person at a gmail account and give them this information:



Full Name:..
Address:..
Nationality:...
Sex:..
Age:..
Phone/Mobile:..
Fax:..
Occupation:..
Company:...
Winning Email Address:.....................................
Reference No:..
Batch No:..
Amount Won:...
Winning Number:...

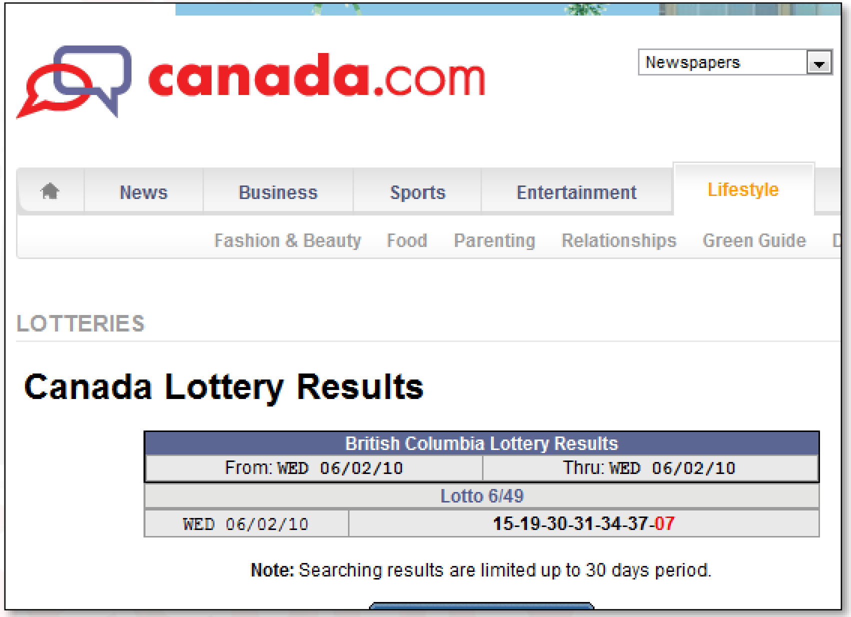
8.3.1. Sample 1: Canadian Lottery

The odd thing is that we should verify the winning number at a website linked at the bottom of the email.

When we open the website, we see that the winning number is:

15-19-30-31-34-37-07

which matches my number!



LOTTERIES

Canada Lottery Results

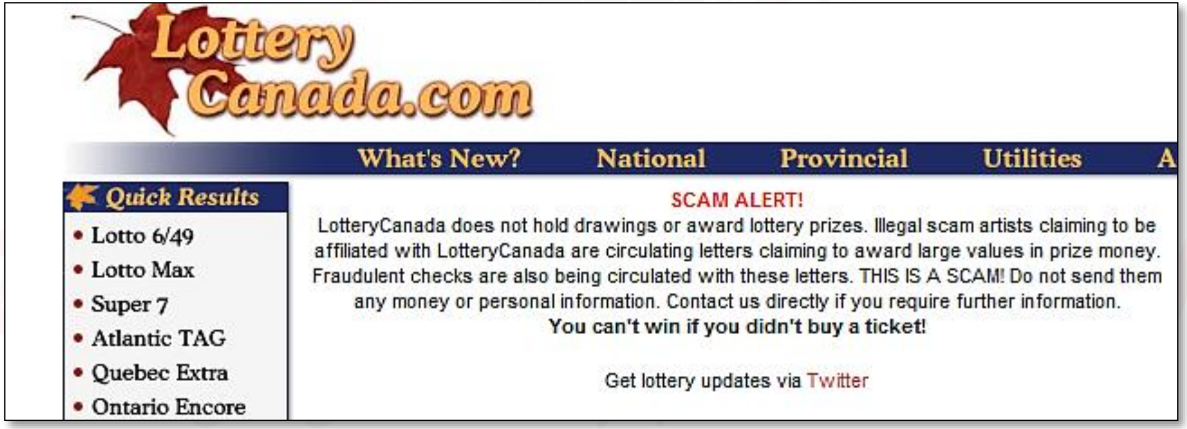
British Columbia Lottery Results	
From: WED 06/02/10	Thru: WED 06/02/10
Lotto 6/49	
WED 06/02/10	15-19-30-31-34-37-07

Note: Searching results are limited up to 30 days period.

8.3.1. Sample 1: Canadian Lottery

So why shouldn't we send this off really quickly so we can get the money?

If we look up the Canadian Lottery rules on their website, it displays this important message right at the top of the screen:



SCAM ALERT!

LotteryCanada does not hold drawings or award lottery prizes. Illegal scam artists claiming to be affiliated with LotteryCanada are circulating letters claiming to award large values in prize money. Fraudulent checks are also being circulated with these letters. THIS IS A SCAM! Do not send them any money or personal information. Contact us directly if you require further information.

You can't win if you didn't buy a ticket!

Get lottery updates via Twitter

8.3.1. Sample 1: Canadian Lottery

Surprisingly enough, we have not bought a lottery ticket.

We just took the most roundabout way to prove that this email was not legitimate, but would most people do the same verification?

Would someone who is suffering financially mind, sending such information just in case they won?

This is exactly what the scammers are hoping.

8.3.1. Sample 1: Canadian Lottery

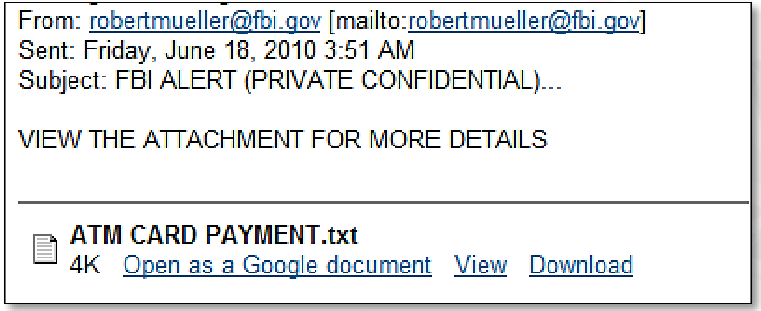
The easiest signs this email was spam, is that it was sent from a Hotmail account, and we were asked to send our information back to a gmail account.

That does not make sense, since lottery Canada has its own domain name, therefore we would think their emails would come from there as well.

Let us now see another example.

8.3.2. Sample 2: FBI E-Mail

Oh no, the FBI has sent me an email!

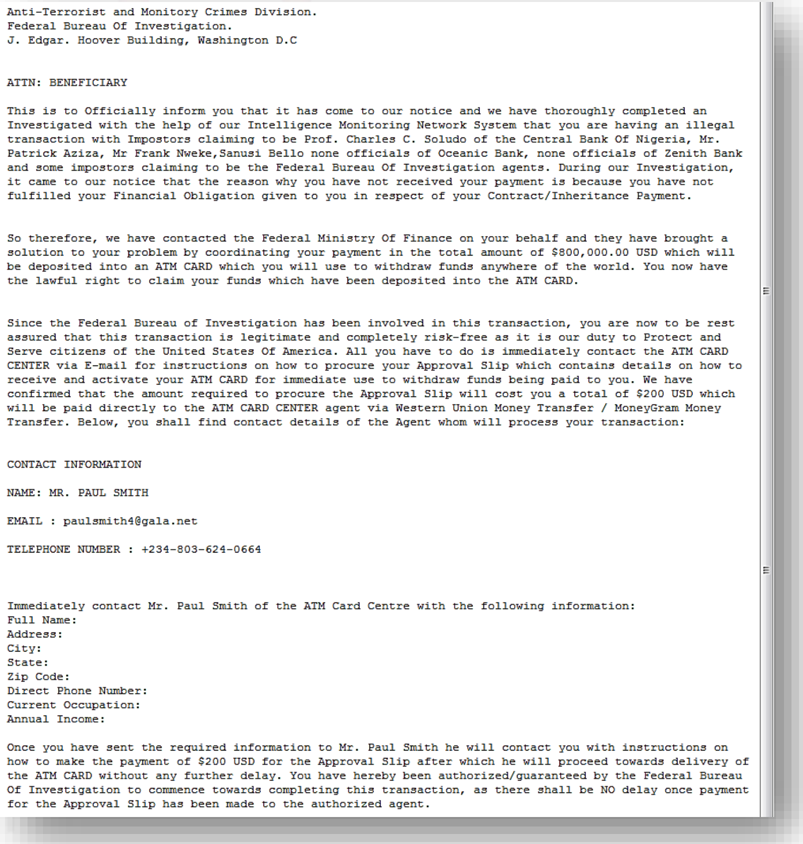


From: robertmueller@fbi.gov [mailto:robertmueller@fbi.gov]
Sent: Friday, June 18, 2010 3:51 AM
Subject: FBI ALERT (PRIVATE CONFIDENTIAL)...

VIEW THE ATTACHMENT FOR MORE DETAILS

ATM CARD PAYMENT.txt
4K Open as a Google document View Download

And the attachment states…



Anti-Terrorist and Monitory Crimes Division.
Federal Bureau Of Investigation.
J. Edgar. Hoover Building, Washington D.C

ATTN: BENEFICIARY

This is to Officially inform you that it has come to our notice and we have thoroughly completed an Investigated with the help of our Intelligence Monitoring Network System that you are having an illegal transaction with Impostors claiming to be Prof. Charles C. Soludo of the Central Bank Of Nigeria, Mr. Patrick Aziza, Mr Frank Nweke,Sanusi Bello none officials of Oceanic Bank, none officials of Zenith Bank and some impostors claiming to be the Federal Bureau Of Investigation agents. During our Investigation, it came to our notice that the reason why you have not received your payment is because you have not fulfilled your Financial Obligation given to you in respect of your Contract/Inheritance Payment.

So therefore, we have contacted the Federal Ministry Of Finance on your behalf and they have brought a solution to your problem by coordinating your payment in the total amount of $800,000.00 USD which will be deposited into an ATM CARD which you will use to withdraw funds anywhere of the world. You now have the lawful right to claim your funds which have been deposited into the ATM CARD.

Since the Federal Bureau of Investigation has been involved in this transaction, you are now to be rest assured that this transaction is legitimate and completely risk-free as it is our duty to Protect and Serve citizens of the United States Of America. All you have to do is immediately contact the ATM CARD CENTER via E-mail for instructions on how to procure your Approval Slip which contains details on how to receive and activate your ATM CARD for immediate use to withdraw funds being paid to you. We have confirmed that the amount required to procure the Approval Slip will cost you a total of $200 USD which will be paid directly to the ATM CARD CENTER agent via Western Union Money Transfer / MoneyGram Money Transfer. Below, you shall find contact details of the Agent whom will process your transaction:

CONTACT INFORMATION

NAME: MR. PAUL SMITH

EMAIL : paulsmith4@gala.net

TELEPHONE NUMBER : +234-803-624-0664

Immediately contact Mr. Paul Smith of the ATM Card Centre with the following information:
Full Name:
Address:
City:
State:
Zip Code:
Direct Phone Number:
Current Occupation:
Annual Income:

Once you have sent the required information to Mr. Paul Smith he will contact you with instructions on how to make the payment of $200 USD for the Approval Slip after which he will proceed towards delivery of the ATM CARD without any further delay. You have hereby been authorized/guaranteed by the Federal Bureau Of Investigation to commence towards completing this transaction, as there shall be NO delay once payment for the Approval Slip has been made to the authorized agent.

8.3.2. Sample 2: FBI E-Mail

The Director of the FBI, Mr. Mueller wants me to send $200 and my personal information to Mr. Paul Smith.

We should rest assured that it is legitimate, since the FBI was involved...(wink, wink)....wait a minute!

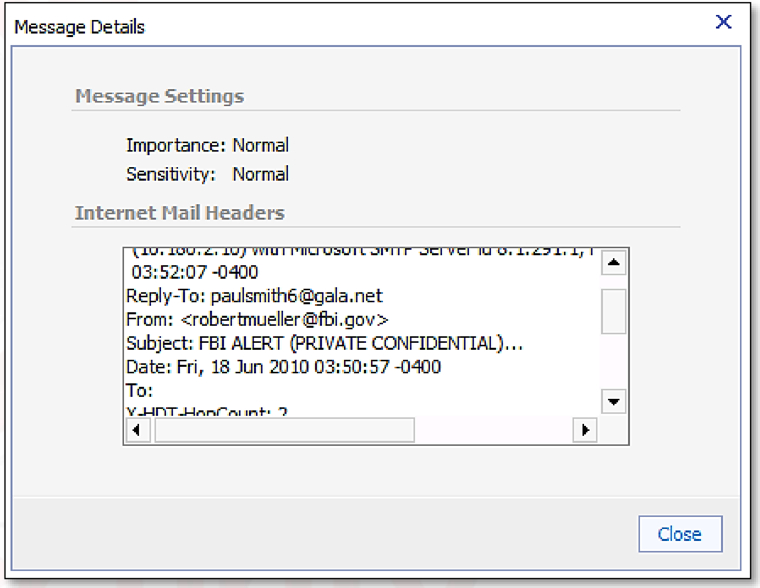
This says the email came from Mr. Mueller at the FBI. We can verify that, by looking at the message headers in the email.

Let’s take a quick look.

8.3.2. Sample 2: FBI E-Mail

According to the headers, the Reply-To: for this message is a paulsmith6@gala.net.

That is funny; we thought we were supposed to send our message to paulsmith4@gala.net. Why would the FBI have me contact a guy overseas to give him $200 and my personal information?



Message Details

Message Settings

Importance: Normal
Sensitivity: Normal

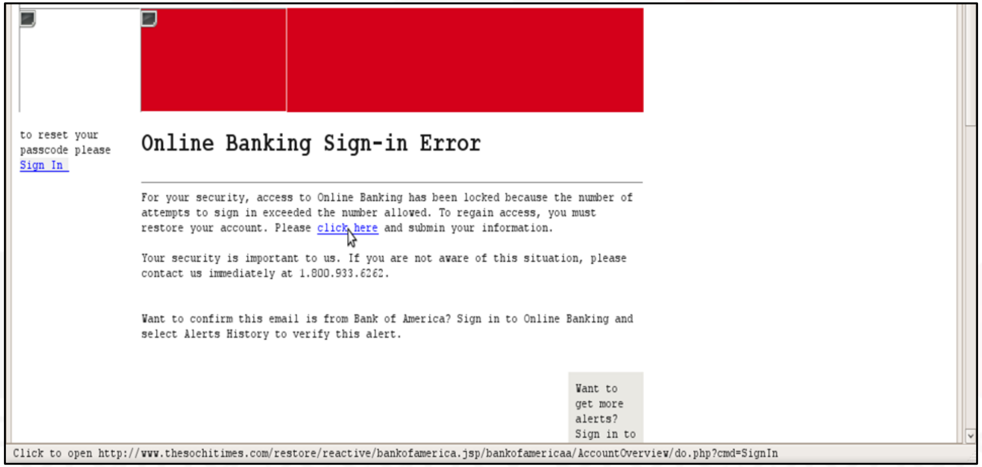
Internet Mail Headers

```
(10.180.2.10) with Microsoft SMTP Server id 8.1.291.1; F
 03:52:07 -0400
Reply-To: paulsmith6@gala.net
From: <robertmueller@fbi.gov>
Subject: FBI ALERT (PRIVATE CONFIDENTIAL)...
Date: Fri, 18 Jun 2010 03:50:57 -0400
To:
X-HDT-HopCount: 2
```

8.3.3. Sample 3: Online Banking

These were just a couple of emails out of my spam folders.

Others emails can be even more convincing, as they have bank logos and official looking content, see below:



to reset your passcode please Sign In

Online Banking Sign-in Error

For your security, access to Online Banking has been locked because the number of attempts to sign in exceeded the number allowed. To regain access, you must restore your account. Please click here and submin your information.

Your security is important to us. If you are not aware of this situation, please contact us immediately at 1.800.933.6262.

Want to confirm this email is from Bank of America? Sign in to Online Banking and select Alerts History to verify this alert.

Want to get more alerts? Sign in to

Click to open http://www.thesochitimes.com/restore/reactive/bankofamerica.jsp/bankofamericaa/AccountOverview/do.php?cmd=SignIn

8.3.3. Sample 3: Online Banking

The site that referenced the pictures has been taken down, but, this email had all of the appropriate Bank of America logos when it was first received.

However, if you notice where the cursor is pointing, the information at the bottom of the screenshot shows you the associated HTML link.

8.3.3. Sample 3: Online Banking

The link does not go to BOA, but to *thesochtimes.com*. This is another way that tricksters can fool the unknowing masses: making the link look official, but redirecting the victim to a page that is owned by them.

The page would look real, but ultimately the person is just giving up their banking information.

Pretexting Samples

8.4. Pretexting Samples

As described in the introduction (to this section) price, pretexting is putting someone in a familiar situation to get them to divulge information.

Let us see some examples in the next slides.

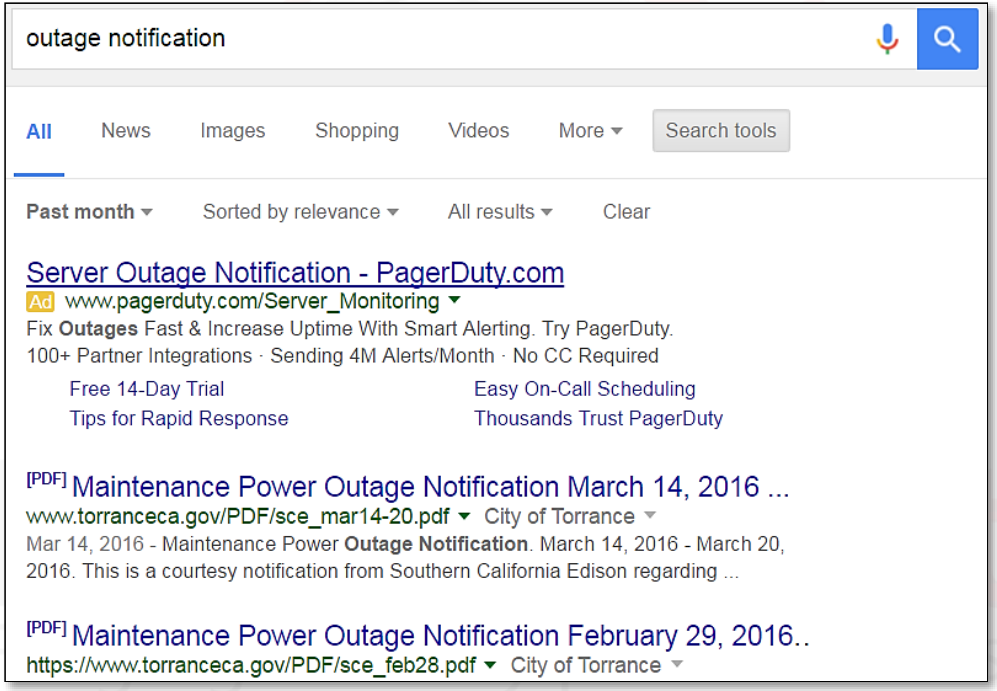
8.4.1. Sample

Let’s say we want to target someone in the general area of an outage that will affect them.

If we go to Google and run a search, like the one showed in the next screenshot, we will get outages posted on different websites.

8.4.1. Sample

Here is a snippet of the results we will obtain.



outage notification

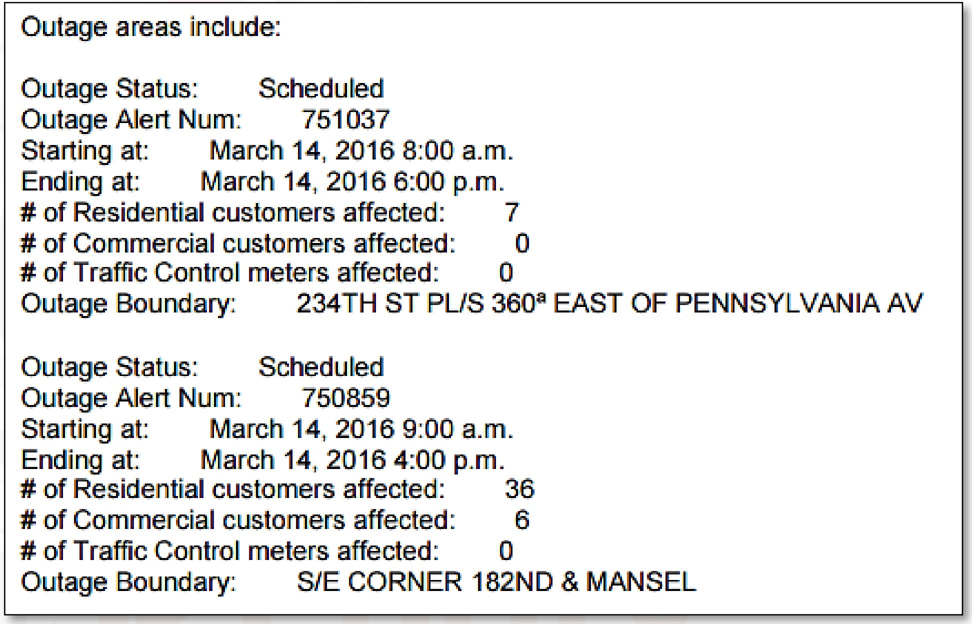
Server Outage Notification - PagerDuty.com
Ad www.pagerduty.com/Server_Monitoring
Fix **Outages** Fast & Increase Uptime With Smart Alerting. Try PagerDuty.
100+ Partner Integrations · Sending 4M Alerts/Month · No CC Required
Free 14-Day Trial
Tips for Rapid Response
Easy On-Call Scheduling
Thousands Trust PagerDuty

[PDF] Maintenance Power Outage Notification March 14, 2016 ...
www.torranceca.gov/PDF/sce_mar14-20.pdf City of Torrance
Mar 14, 2016 - Maintenance Power **Outage Notification**. March 14, 2016 - March 20, 2016. This is a courtesy notification from Southern California Edison regarding ...

[PDF] Maintenance Power Outage Notification February 29, 2016..
https://www.torranceca.gov/PDF/sce_feb28.pdf City of Torrance

8.4.1. Sample

Once opened, we see that there will be power outages in specific areas.



Outage areas include:

Outage Status: Scheduled
Outage Alert Num: 751037
Starting at: March 14, 2016 8:00 a.m.
Ending at: March 14, 2016 6:00 p.m.
# of Residential customers affected: 7
# of Commercial customers affected: 0
# of Traffic Control meters affected: 0
Outage Boundary: 234TH ST PL/S 360ª EAST OF PENNSYLVANIA AV

Outage Status: Scheduled
Outage Alert Num: 750859
Starting at: March 14, 2016 9:00 a.m.
Ending at: March 14, 2016 4:00 p.m.
# of Residential customers affected: 36
# of Commercial customers affected: 6
# of Traffic Control meters affected: 0
Outage Boundary: S/E CORNER 182ND & MANSEL

8.4.1. Sample

Knowing this, we can open Google Maps and take a look at the area, the address and eventually find the owner of one of the locations.

So, in 15 minutes or less, we will have enough information to construct our pretexting attack.

So, let us create our script.

8.4.1. Sample

The following is an example of what our conversation may look like:

Hello Mr. Gerhard, My name is John Townsend from Southern California Edison and need to speak with you about some upcoming changes in your area. First I need to verify some information from you to validate that you are the right person I should be speaking with, you know you can never be too careful these days.

First can you repeat your name and address for me?

Great! That much I have correct! Now can you tell me the last 6 digits of your Social Security Number?

Note that I'm not asking for your whole SSN, just the last 6 so we can ensure it is you without having all the numbers.

Getting close now Mr. Gerhard, just a couple more questions.

What is the state you were born in?

Continue...

8.4.1. Sample

May I have your Date of Birth?

And do you use Oxygen or any other medical equipment that requires your power to always be on?

Excellent Thanks! We at SoCal Edison thank you for your patronage and want to inform you that you are going to be having a community power outage on June 27th from 9am to 6pm. We want to ensure that you are aware of this if you need to make any arrangements for a cool place to go, or to ensure that any medical equipment is sufficiently accounted for power wise as this outage will be prolonged.

I want to thank you for your time today, Mr. Gerhard, and thanks again for being a SoCal Edison Customer…..Have a Great Day!!!

8.4.1. Sample

So, in a relatively short amount of time, we have constructed a believable story and found a suitable victim.

So what did or did not we get?

Well, note that we did not ask for the full Social Security Number, but we did get the last 6 numbers, plus the state in which the person was born.

8.4.1. Sample

Every state has a set of prefixes, that is used for Social Security Numbers. Now, all we have to do is reference that list and we will obtain the full SSN! Here is a list.

As you can see, a little bit of internet searching and some creative thinking, is all we need to try and find unwitting victims.

https://www.einvestigator.com/social-security-numbers-ssn/

8.4.1. Sample

Now keep in mind that this is illegal since the adoption of the Gramm-Leach-Bliley Act of 1999, which makes it illegal to:

- Use false, fictitious or fraudulent statements or documents to get customer information from a financial institution.
- Use forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Ask another person to get someone else's customer information using false, fictitious or fraudulent statements or using false, fictitious or fraudulent ...

8.4.1. Sample

Governments are familiar with these scams, but it is not always easy to find and prosecute scammers.

Therefore, we have to rely on the victim education, to ensure that they are not taken advantage of in these types of scenarios.

Tools

8.5. Tools

During the years many tools have been developed to help and improve social engineering attacks.

Tools can help to generate fake links, fake pages, social sharing campaigns and much more.

The one we are going to explore in the coming slides is called Social Engineer Toolkit (SET).

https://github.com/trustedsec/social-engineer-toolkit

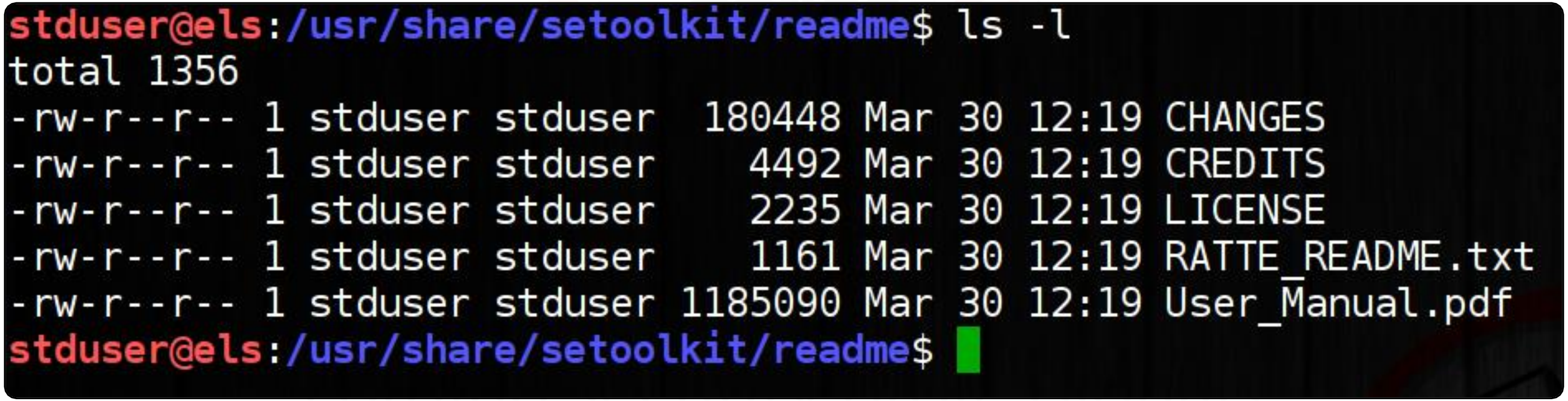
8.5.1. SET

As stated on its website: "*The Social-Engineer Toolkit is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack quickly*".

As you will see, it can be used to create phishing pages, bind Metasploit exploits, create fake emails and much more.

8.5.1. SET

Before actually using the tool, we strongly suggest you read its user manual. You can either read it at the following link or you can find it in the installation folder of SET (within the readme folder):



```
stduser@els:/usr/share/setoolkit/readme$ ls -l
total 1356
-rw-r--r-- 1 stduser stduser  180448 Mar 30 12:19 CHANGES
-rw-r--r-- 1 stduser stduser    4492 Mar 30 12:19 CREDITS
-rw-r--r-- 1 stduser stduser    2235 Mar 30 12:19 LICENSE
-rw-r--r-- 1 stduser stduser    1161 Mar 30 12:19 RATTE_README.txt
-rw-r--r-- 1 stduser stduser 1185090 Mar 30 12:19 User_Manual.pdf
stduser@els:/usr/share/setoolkit/readme$ 
```

https://github.com/trustedsec/social-engineer-toolkit/tree/master/readme

8.5.1. SET

As you will see in the user manual PDF, before using SET you probably will have to configure a few settings such as: Metasploit folder, HTTP server options, SSL certificates…

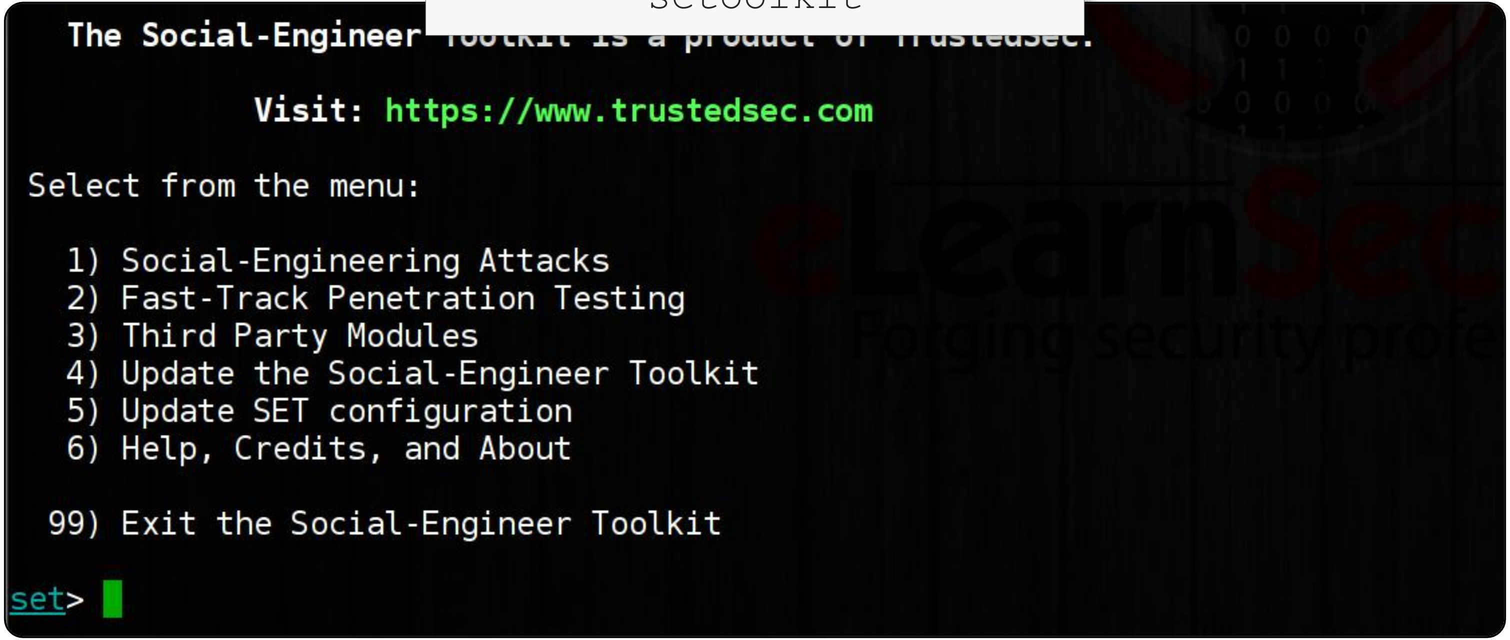
Once again, we strongly suggest you go through the user manual and read the "*Beginning with the Social Engineer Toolkit*" section.

8.5.1. SET

MAP REF

To start using SET, we can run the following command:

```
setoolkit
```



```
   The Social-Engineer Toolkit is a product of TrustedSec.

             Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

8.5.1. SET

As you can see form the previous screenshot, SET is very easy to use. We just need to select what to do from the menu printed in the console.

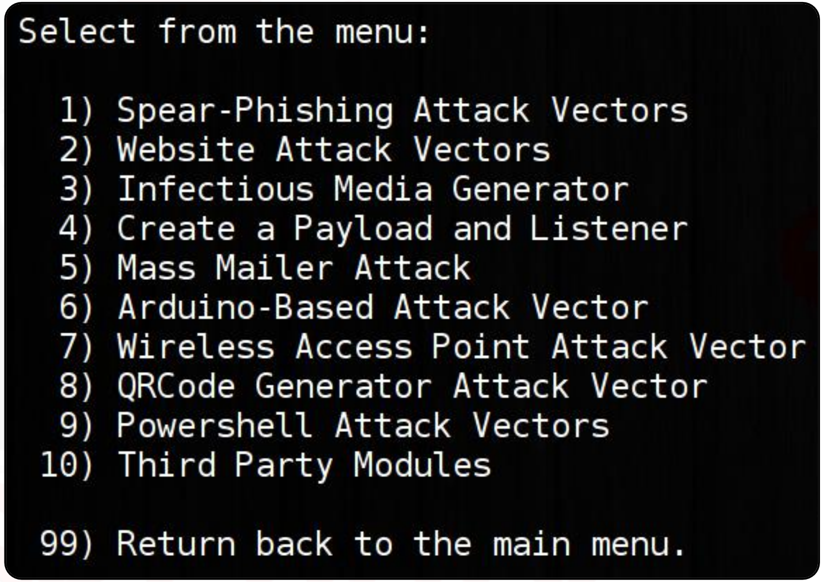
The Social-Engineering Attacks menu contains all the modules that help us in configuring attacks such as spear phishing, infecting media (USB/CD/DVD), sending mass mail and much more.

The Fast-Track Penetration Testing contains modules that help us in the automation of complex attack vectors.

8.5.1. SET

Let us now start a social engineering attack and see what modules SET offers. In the previous menu, we will select the option number 1.

The screenshot shows all the attacks that we can run.



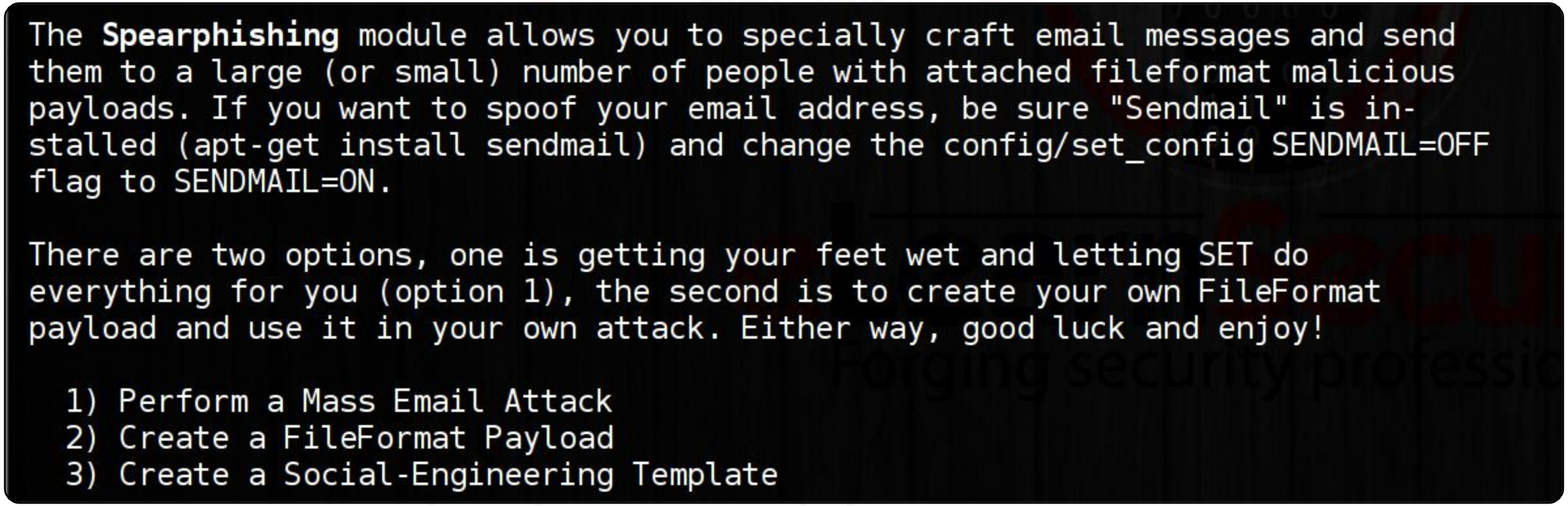
```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.
```

8.5.1. SET

Notice that we can acquire more information about each attack vector by simply selecting it. For example, if we type 1 and confirm, we will see the following message:



```
The Spearphishing module allows you to specially craft email messages and send
them to a large (or small) number of people with attached fileformat malicious
payloads. If you want to spoof your email address, be sure "Sendmail" is in-
stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do
everything for you (option 1), the second is to create your own FileFormat
payload and use it in your own attack. Either way, good luck and enjoy!

  1) Perform a Mass Email Attack
  2) Create a FileFormat Payload
  3) Create a Social-Engineering Template
```

8.5.1. SET

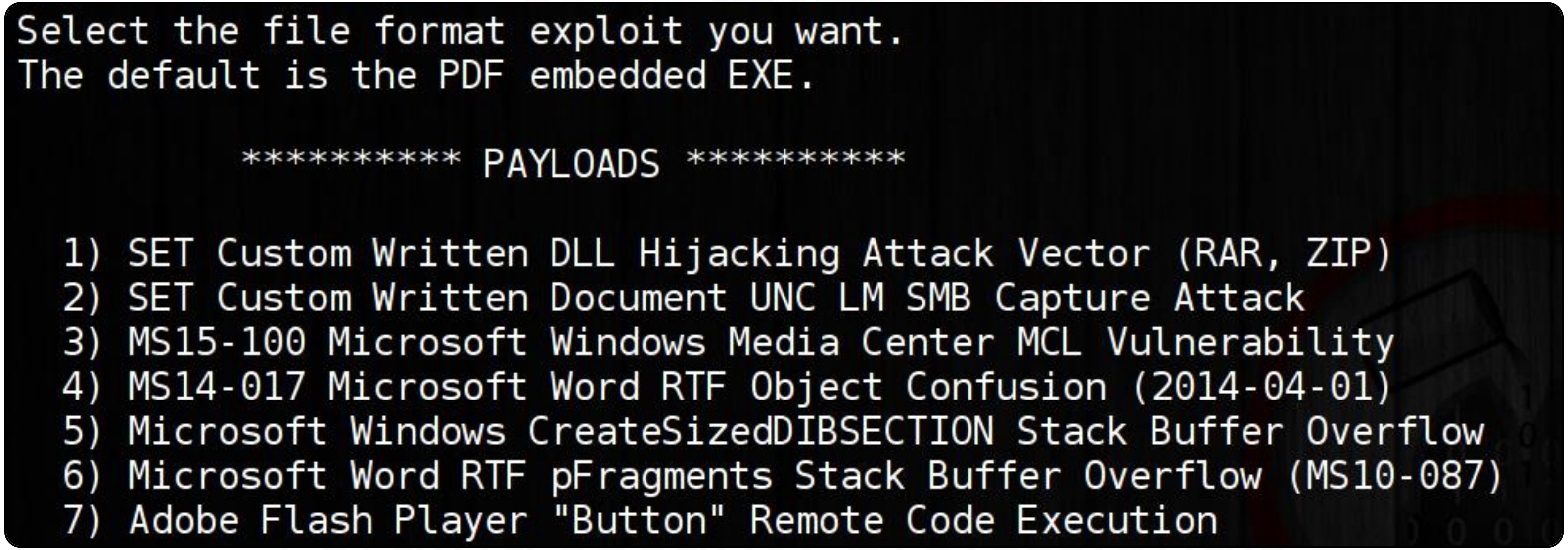
As you can see, using SET is very straightforward. We just need to select the modules we wish to use and configure them step by step.

Also notice that each module and each attack vector is different, thus the options to set will be different.

Let’s now select the first option (*Perform a Mass Email Attack*) and see what we get.

8.5.1. SET

In the next output, SET asks us to select the type of exploit we want to use in the email. As you can see it offers many different exploits, but we can also use custom executables.



```
Select the file format exploit you want.
The default is the PDF embedded EXE.

          *********** PAYLOADS ***********

  1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
  2) SET Custom Written Document UNC LM SMB Capture Attack
  3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
  4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
  5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
  6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
  7) Adobe Flash Player "Button" Remote Code Execution
```

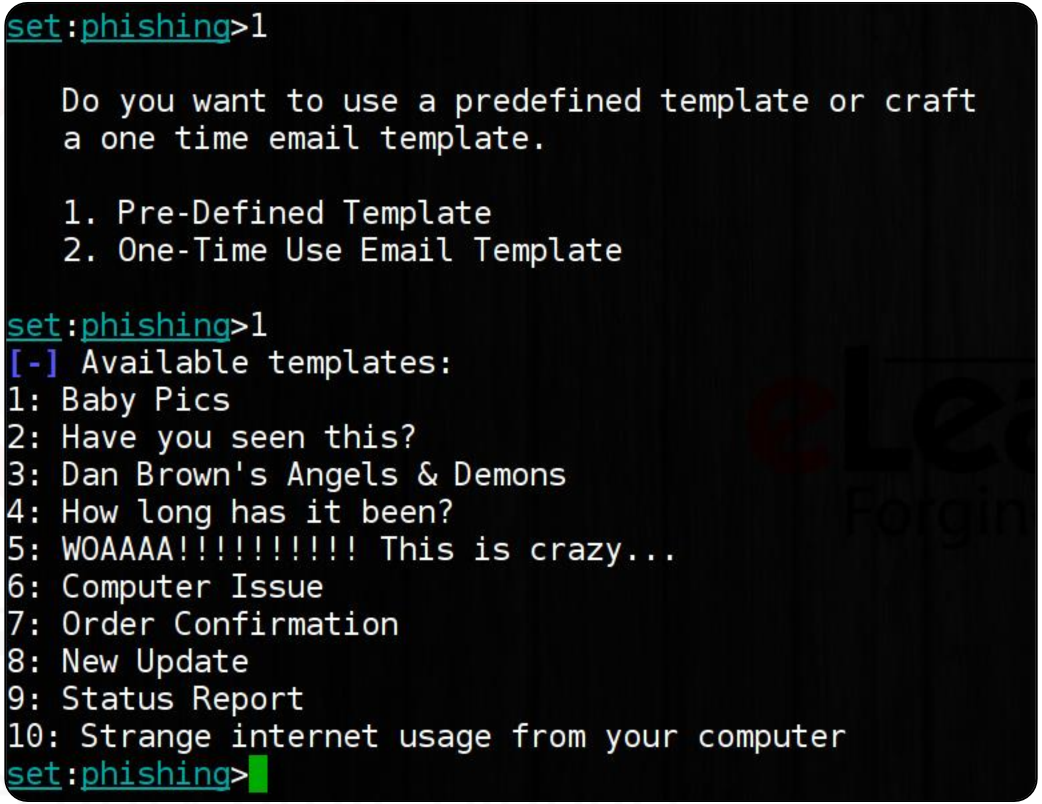
8.5.1. SET

Once we have selected the exploit to use, we will continue configuring our attack. For example, we have to choose the type of payload we wish to use (meterpreter, SET interactive shell and so on).

After that, we will also have to configure the target email address, the template to use and the SMPT configuration to send the phishing email.

8.5.1. SET

As we can see in the screenshot, SET allows us to use either predefined templates or custom ones.



```
set:phishing>1

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Baby Pics
2: Have you seen this?
3: Dan Brown's Angels & Demons
4: How long has it been?
5: WOAAAA!!!!!!!!!! This is crazy...
6: Computer Issue
7: Order Confirmation
8: New Update
9: Status Report
10: Strange internet usage from your computer
set:phishing>
```

8.5.1. SET

As already stated, depending upon the attack selected, all the configurations that follow will change accordingly.

Exploring all the attacks and their settings during this course is impossible. We strongly suggest you use SET and navigate its options, in order to test its power and flexibility.

Social Engineering for Linux Targets

REFERENCES

References

Virus Total

http://www.virustotal.com/

Social Engineering Toolkit

https://github.com/trustedsec/social-engineer-toolkit

LinDrop

https://www.obscurechannel.com/x42/lindrop.html

SSN

http://www.einvestigator.com/links/social_security_numbers.htm