Telephone-based Social Engineering Script EN

Jan-Willem Bullée
j.h.bullee@utwente.nl

Script

Hi this is [name].

We discovered that the PC you are using is distributing spam emails. This is caused by a malicious program that is running in the background.

Q: Did you notice that your PC was a bit slower lately?
Y: this is one of the side effects.
N: lucky you, usually this is one of the symptoms.

There is nothing to be ashamed of, there are other people who have the same problem. I already helped 3 people to fix this earlier today. Luckily this is easy and quick to solve.

Q: Do you have 2 or 3 minutes, so we can remove it together right away.
Yes: Continue  No: Better solve it now, then you can continue your daily business.
Yes: Continue  No: It is only 2 or 3 minutes
Yes: Continue  No: Can I call you later today?
Yes: Call back  No: Early termination.

Please open an internet browser and type the following URL in the address bar:
URL: “http://spam.utwente.info”

To continue the download procedure, please enter the validation code, this is your complete employee number.
Counter Question: I only know 7 digits.
A: The complete can be found on your employee card.

Please save the file to your Desktop and execute it.
Q: After the program is finished, could you read out the completion code?

DEBRIEF.
Thank you for your cooperation. I would like to explain something about our procedure. We are training staff to increase awareness to fraud. I am a bachelor/master student performing research fraud prevention. This training is organised by Jan-Willem Bullée (who is a PhD candidate in the EWI-SCS chair at the University of Twente) and in collaboration with the management of the University.

What just happened was a preventive training. We do this to simulate telephone calls that might be executed by a real attacker. We do this to increase awareness of the university staff. It is important to do these exercises because most people have a natural tendency to be helpful to others. The unfortunate thing here is that offenders also know this and will exploit this in their own benefit. Offenders will try to gain your trust by using a false identity and a credible story. They try to obtain valuable information or make you perform actions or your PC. This is called Social Engineering.

There are some indicators that suggest something is going on. i) The originator of the call uses an ‘anonymous’ number; ii) You are asked via the telephone to do something on your PC; iii) The website looks like the trusted website, but is slightly different. When you think that something is going on, challenge the requester to validate this/her identity. Furthermore, you can do a call back, using a known and trusted number.

To prevent staff from falling for those attacks, we execute this sort of trainings - in collaboration with the management of the University.

For our understanding I have some questions regarding what just happened.

Is this OK with you?

Everything you say is and will be treated as confidential. The outcome will be anonymized, combined with others and subjected to statistical analysis.

Do you agree on this?

Before we continue, I would like to ask you not to share the design and contents with other employees or colleagues. This is really important for us. Is this all right with you? If there are any questions, please contact the leader of this training, Jan-Willem Bullée.
Early Termination (STOP)

Thank you for your cooperation, you did an excellent job by not blindly following my instructions. Well done. As you probably already figured out; I tried to con you.

I would like to explain something about our procedure. We are training staff to increase awareness to fraud. I am a bachelor/master student performing research fraud prevention. This project is organised by Jan-Willem Bullée (who is a PhD candidate in the EWI-SCS chair at the University of Twente) and in collaboration with the management of the University.

What just happened was a preventive training. We do this to simulate telephone calls that might be executed by a real attacker. We do this to increase awareness of the university staff. It is important to do these exercises because most people have a natural tendency to be helpful to others. The unfortunate thing here is that offenders also know this and will exploit this in their own benefit. Offenders will try to gain your trust by using a false identity and a credible story. They try to obtain valuable information or make you perform actions or your PC. This is called Social Engineering.

There are some indicators that suggest something is going on. i) The originator of the call uses an ‘anonymous’ number; ii) You are asked via the telephone to do something on your PC; iii) The website looks like the trusted website, but is slightly different. When you think that something is going on, challenge the requester to validate this/her identity. Furthermore, you can do a call back, using a known and trusted number.

To prevent staff from falling for those attacks, we execute this sort of trainings - in collaboration with the management of the University.

For our understanding I have some questions regarding what just happened. Is this OK with you?

Everything you say is and will be treated as confidential. The outcome will be anonymized, combined with others and subjected to statistical analysis. Do you agree on this?”

Before we continue, I would like to ask you not to share the design and contents with other employees or colleagues. This is really important for us. Is this all right with you? If there are any questions, please contact the leader of this training, Jan Willem Bullée.
Difficult questions + answers

1. Why are you calling me, couldn’t this be done automatically?
   *It is only a limited amount of users, ringing these few individuals is quicker than preparing it for centralized distribution.*

2. The application does not launch on OSX.
   *Press *command* + [space] type “security” this will open a new screen called “Privacy and security” click on ‘launch anyway’*

3. On behalf of whom are you calling?
   *Early termination*

4. Who is your supervisor?
   *Early termination*

5. Why can’t I see your phone number?
   *Sorry, I have no idea.*

6. How did I got this (spam distributing) program?
   *Probably via an infected mail or website.*

7. Which program in particular is distributing the spam from my computer?
   *It seems to be a newly discovered malware program, I have no detailed knowledge regarding technical details of this malware program.*

8. Why do you need my employee number?
   *We need this to close the incident report.*

9. Why do you need this completion code?
   *We need this to validate that the removal was successful.*