

Practise What You Preach: a study on tech-savvy readers' immunity to social engineering techniques

Sabina DATCU, Ioana JELEA

sdatcu@bitdefender.com

ijelea@bitdefender.com

Table of Contents



1. Introduction
2. Methodology
3. Analysis
 - 3.1. Qualitative analysis
 - 3.2. Quantitative analysis
4. Results and Discussions
5. Conclusions

Introduction

Social Engineering

- process of deceiving people into giving you access to confidential information
- an art, a combination of creativity and skill.



Introduction

Social Engineering

- each attack has its unique features

BUT...

- they all tend to follow the same steps:

information gathering



relationship development



exploitation



implementation.

Introduction

- the number of articles, news reports, stories connected to “cyber-security” is greater than before

SO...

- the number of “security-savvy users” has increased considerably

BUT...

- scammers are still doing their jobs very well due to inherent human weaknesses -> directly linked to the psychological and emotional background of the targeted persons



- 2 types of analysis: qualitative and quantitative
- **Qualitative analysis** – The Health Belief Model (HBM), Theory of Reasoned Action; Personal or Moral Norms, Persuasive Communication, Identity Theory, Risk Homeostasis
- **Quantitative analysis** – 643 “security-savvy users” interviewed



QUALITATIVE ANALYSIS



Aim:

- to identify situations in which tech-savvy commentators/forum members willingly break/testify to having broken data security rules they are well aware of
- to test the explanatory models against rule-breaking situations that are relevant to online safety
- to “measure” the distance between norm and action

Theoretical background - Summary



- 1. Health Belief Model (HBM)**- desire to avoid an incident (infection, data theft, breach of privacy) vs belief that a prescribed action will prevent the incident
- 2. Theory of Reasoned Action – personal or moral norms:** users continue interacting with an unknown person even when the suspicion of a scam has already arisen
- 3. Persuasive Communication – “*who says what to whom*”;** linguistic clues why users manage/do not manage to avoid scam traps
- 4. Identity Theory** - membership into a specific online community perceived as rendering individuals immune to security risks
- 5. Risk Homeostasis – level of acknowledged risk:** users engage in potentially dangerous interactions to test opponents’ technical knowledge and skills

QUALITATIVE ANALYSIS



What defines tech-savvy users here:

1. they **read and comment** on news pertaining to the data security industry/ know about and communicate on tech support forums
2. **demonstrate some degree of data security knowledge** (awareness of the existence of scams and of scam proving methods, awareness, even post factum, of social engineering techniques)

QUALITATIVE ANALYSIS



Typology of analyzed situations based on:

1. *perceived likelihood* of a data security incident versus *action* taken to prevent it
2. *personal norms* preventing action in interactions posing a data security risk
3. perceived elements of *persuasive communication* versus reasons why such elements were ignored
4. *acknowledged degree of risk* taken in interactions/incidents posing a data security risk.

QUALITATIVE ANALYSIS



June 6th, 2011, 12:53 PM #22

Infrequent Poster Join Date: Jun 2011 Posts: 1

Re: Ammy Scam

i just got a call from a HINDI GUY at AMMY named "Bob Garrett". he ran me through his spiel and tried convincingly to get my information to which i folded... i didnt immediately suspect anything until i thought about it and replayed the conversation in my head... when i answered the phone he asked for me by name...wth?? i have a paypal...rather i HAD a paypal acct... couldnt figure out how to close it so i quickly called my bank and got my acct. # changed.

do not trust anyone who claims to know anything about your computer when your sitting right in front of it and notice not a thing wrong. i was a fool and fell for their scam but fortunately they will not be getting this fool's money. i am forever scanning my computer - everyday and several times a day. i was scared. i panicked. but thank god i realized what was up before any damage was done. on another note, when BOB told me to access the ammy.com, i instead went uninstall utorrent.org which i believed was the problem. while i was uninstalling said torrent, BOB asked me what i was doing... i claimed my computer froze. a few seconds later he asked "what are you doing? why is it taking so long?" ... claimed i was still frozen.... had i been more aware at the time i would have google for the ammy scam firstly before allowing that asshole any information or access.

the number that appeared on my phone is 1-760-705-8888. i called the number and it cannot be accessed.

if anyone from that number or any other contacts you for any information DO NOT FALL FOR IT!!! these ppl are cruel, malicious beasts with no conscience. something needs to be done about these bastards...if the authorities refuse to stop them it is up to us.

ps "BOB" said i need to 'remove viruses from all the layers of my computer', then purchase 'microsoft virus removal', hard disc platter recovery software', a 'licensed version of firewall' (helloooo i have anti malware and firewall already installed!!). also he told me to purchase a 'ready start version of avast' and if possible to hire a microsoft engineer to 'fix the problems'. with the exception of the hiring a 'microsoft engineer' the programs would cost me a grand total of \$186 canadian dollars.

as an after thought, he also asked if i have a cell phone to contact me if im out...thankfully i had none to give him otherwise he'd be pestering me there as well. he also claimed that if i don't fix my computer it will crash in 3 hours???

pps i was reading several of these postings to my sister and she told me that she got a cold call from these ppl as well...several months ago, claiming that her computer was infected and immediate action needs to be taken to rectify the issues... needless to say that she was more than a bit confused by that seeing that she hasnt had a computer in almost 4 years...

@ "The guy sounded like he was actually in a call center and he was very confident in his manner about getting me to my computer"... i noticed that to a degree as well. though my guy distinctly sounded as though he was in a very large warehouse. also i noticed a constant beeping amongst other voices in the background.

lastly i would like to mention to each and everyone in here that if you ever receive a "courtesy call" from your bank or service provider i will advise to to immediately hang up and call back whomever the caller claimed to be working for the verify the information.

Last edited by : June 6th, 2011 at 01:36 PM.

Perceived likelihood of incident- low -> No action

I didn't immediately suspect anything; the guy sounded he was actually in a call center and he was very confident in his manner -> I noticed that to a degree, but....

The victim attempts to question the veracity of the caller's claim, but fails to take action in the first place because of the caller's position of authority as support center representative

QUALITATIVE ANALYSIS



July 10th, 2011, 09:29 AM #31

Infrequent Poster

Join Date: Jul 2011
Posts: 1

Re: Ammyy Scam

I received a phone call yesterday. It was from an Indian sounding woman, she said she was working for Microsoft and my pc was full of viruses, she said she could show me the viruses, I was very concerned but she was very convincing, she told me to type Ammyy web address in to my browser, which I did, I even asked her if this was genuine and of course she said yes. She then handed the phone to her "supervisor" who was an Indian sounding man. He said he would show me where the infection was, he also told me to open notepad and typed in 3 different things that they could supposedly download to fix my computer and that they would send me the activation keys as apparently in the UK you need to do this by law. At this point I asked if this was going to cost me and he says it was free, then added there would be a one off payment of £79. Immediately I said, my husband will have a fit, and closed down my pc. (a bit slow on the uptake maybe but they were very convincing.) I actually felt sick, I ran a full system scan and no virus or anything were fine, hope all will be ok as they have my name, address and e-mail address, can't believe how stupid I was!

Personal norm helps the victim decide against the course of action suggested by the scammer.

When asked for a 79£ payment, the victim puts an end to the conversation for fear of her husband's reaction to her making such an expense.

August 6th, 2011, 11:42 AM Thread Tools Search this Thread #51

Infrequent Poster Join Date: Aug 2011
Posts: 1

Re: Ammy Scam

So I got the call in Canada at 9:30 last night just like most of you. I figured the guy was a scam but decided to follow him through till he tried to sell me something or do something really suspicious. Anyways he started out as "Greg Stone" and got me to search for error reports on my computer yada yada yada. 47,000 errors or what ever. He goes on saying I'm in grave danger and my computer is going to crash and be completely corrupted and not fixable if i wait. so I being young and stupid went through with the scam process and let him remotely access my computer ☺ . As he asked me to type into my run box certain commands I just closed every window that was currently open and find someone madly typing(from a remote location) commands into a notepad type window. suspicious yes I know. what's even more suspicious was that they were typing; error:985236...98.56% files corrupt...-www.megabitessolutions.com- ...only solution is to download unlimited service... and some more junk like that. So they close their box and ask me to retry my scan which i do. Ironic enough at the bottom of my new search for corruption comes the exact same message that he was typing... Since when did windows Preload the message the if you have so many errors the only solution is to buy this one fix-all program. anyways it was over 200 dollars canadian so i straight up told him i couldn't make the purchase since I'm "under 18" and needed to wait till my parents are home. he wasn't very happy with that but said i needed to do it as soon as they got home. He told he he's going to call back on monday (highly doubt it!!) and i asked him if i had "trouble" if i could call him so he gave me his number (I highly doubt it's correct at all but here it is) 307-529-0607 and his name is now Steve Carter haha.

What the really concerning thing is how the hell did they get my computer ID, name, phone number, and he claimed to have my email too. Well done Windows, your security is really doing a good job of protecting my privacy.

Subjective level of risk accepted in cases where the suspicion of scam arises.

The forum member starts by saying that he willingly followed the unknown caller's directions "till he tried to sell me something or do something really suspicious".

QUALITATIVE ANALYSIS



Member with 10,351 posts. Join Date: Jan 2003
Experience: Intermediate
25-Mar-2012, 05:58 PM #4

Sure you can have my Facebook name and password. Oh, that's right I don't have one, I gave up on Facebook a long time ago, figuring things like this would happen.

Moderator & Malware Removal Specialist with 38,392 posts. Join Date: Dec 2002
Location:
25-Mar-2012, 06:05 PM #5

Quote:

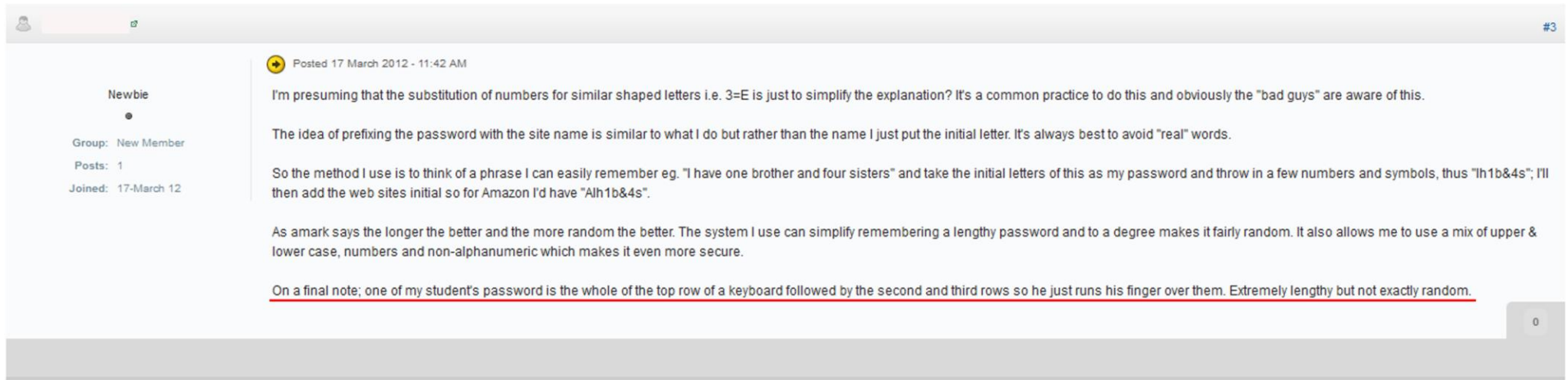
Originally Posted by [redacted] [View Profile](#)
Sure you can have my Facebook name and password. Oh, that's right I don't have one, I gave up on Facebook a long time ago, figuring things like this would happen.

oh you do still have one

Facebook NEVER delete accounts only make them inactive & the log in you had will still work, even if you haven't used it for years or have asked them to delete it

Distance between rule and action under rule; Low perceived risk -> no preventative action plus extra info volunteered

The forum member initially acknowledges the risk posed by password sharing, but chooses to disregard it, which leads to his/her being exposed as not having a very clear idea about a social network account's closedown.



The screenshot shows a forum post from a user named 'Newbie'. The user's profile information on the left indicates they are a 'New Member' with 1 post and joined on 17-March 12. The post itself, dated 17 March 2012 at 11:42 AM, discusses password creation techniques. It mentions the substitution of numbers for similar letters (e.g., 3=E), the use of site names as prefixes, and a method of using a memorable phrase like 'I have one brother and four sisters' to generate a password. The user also notes that longer and more random passwords are better and that their system allows for a mix of upper and lower case, numbers, and non-alphanumeric characters. A final note, underlined in red, states: 'On a final note; one of my student's password is the whole of the top row of a keyboard followed by the second and third rows so he just runs his finger over them. Extremely lengthy but not exactly random.'

**Distance between rule and action under rule;
Low perceived risk -> no preventative action plus extra info volunteered**

Commenting on an article advising readers on how to create a strong password, the user ends up revealing his own version of a password creation mechanism.

I will state this once again. I have been a Mac user since 1985. Since then I have worked at many Mac-only advertising agencies and most of my friends are designers & writers who use Mac's in their personal lives as well as work lives. And I have never known one single Mac user who has ever had a computer virus, trojan horse, or malware. Conversely I've only met a few PC users who haven't had such problems.


Posted by  (78 comments)
May 21, 2012 9:11 AM (PDT)

 Like (4)  Reply  Link  Flag

The difference is...you and your associates seem to be more intelligent than most others and would use the computers more responsibly while surfing the web.

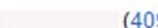
I, conversely, us PCs and have never had a virus/trojan because I know what I'm doing. Although, I know they exist.

Just because you haven't seen it doesn't mean it doesn't exist.

Posted by  (908 comments)
May 21, 2012 12:05 PM (PDT)

 Like  Link  Flag

The best protection against malware and viruses on any system is the user. The user being careful. The problem with people thinking they are safe because of the hardware is that they will fall for stupid things. Don't buy antivirus, just be informed and careful. Same is true on Mac or Windows.

Posted by  (4092 comments)
May 21, 2012 9:32 AM (PDT)

 Like (1)  Reply  Link  Flag

Constructed identity and objective rule vs personal norm

A form of prescribed conduct – *use of an antivirus on Mac devices*- is broken due to the existence of a subjective reason– *I have not seen this happening to anyone around me*– strengthened by the respective person's membership in a group considered to be immune to risks – *Mac users never get infected*.

Hypotheses :

H1: The **higher** the interviewees' security/privacy **knowledge**, the **stricter** their **attitude**/conduct towards privacy.

H2: The **more** interviewees **use the Internet to impress the others**, the **less strict** they are about the privacy of their data.

H3: The **higher** the **level of** interviewees' **narcissism**, the **less strict** their attitude about private information disclosure.

QUANTITATIVE ANALYSIS

SURVEY:

- 643 tech savvy users
- time frame: 2 months

-Narcissism – ‘I am an extraordinary person, I deserve a lot of attention’

| <i>Information disclosed</i> | <i>%</i> |
|---|----------|
| <i>Personal information</i> | |
| Address and phone | 94 |
| Parents' names | 81 |
| Information about their family | 80 |
| <i>Job/Interests</i> | |
| Strategies, future plans | 97 |
| Information about co-workers | 93 |
| Information about the company they work for | 91 |
| <i>Passwords</i> | |
| Type of passwords | 82 |
| Other info about their passwords | 53 |
| <i>Image for the others</i> | |
| Others' opinions about them | 96 |

NARCISSISM



- could predict the likelihood of users protecting their sensitive data.
- related to presenting oneself positively in front of a large audience



If users are admired and appreciated by the others, they enthusiastically disclose a lot of sensitive information in the discussions.

CONCLUSIONS



- Low levels of perceived risk or a specific degree of acceptable risk, personal norms, membership in a community, persuasive communication may cause users to break security rules they are aware of.
- The distance between prescribed and actual action depends on the salience of one or several of these elements – personal “gullibility” factor
- The experiment revealed interesting results, but it certainly does not provide the last word in the privacy debate.

Thank You!