

The Psychology of Scams and Malware in Social Media

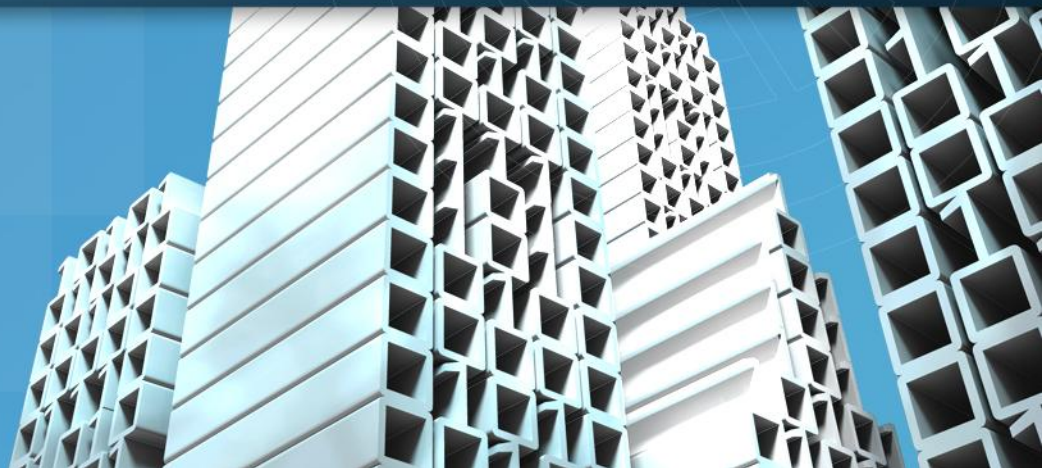
Amon Sanniez
Security Researcher WSL

TRITON™

Web security

Email security

Data security



2008



Facebook

In May 2008 a bug in Facebook's friend optimization algorithm showed the top 5 viewers of your profile



Facebook

In December 2008 Koobface first appears



Twitter

In August 2008 malicious erotic ads infected users with a trojan-downloader masquerading as an Adobe Flash update

2009



Facebook

In August 2009 the first "Profile Spy" app appears – Stalker Check



Twitter

In April 2009 XSS worm "Mikey"



Twitter

In February 2009 clickjacking proliferates



Myspace

In 2010 Myspace suffered from Phishing emails pretending to be from Myspace support asking end users to reset their password



Facebook

In May 2010
"likejacking" begins....



Facebook

In October 2010
Firesheep

2010



Twitter

In September 2010 a "MouseOver" exploit is discovered which could infect users without them even clicking on the link

- A fraud or a scam could also be defined as *an illegal marketing offer* (Fischer, Lea, & Evans, 2008)
- The four P's of the marketing mix apply (Product, Price, Place, Promotion) (McCarthy, 1960)
- To simplify – a scammer sells the *mark something* and they buy it.
- *Fraudem (Latin)* - deceit or injury (Simpson & Weiner, 2009)
- *Scam* – Probably first used by actor Steve McQueen in 1963 in a Time Magazine interview (Luce, 1963)

- Money is being lost (£9.3 billion in 2009 in UK lost to 419 scams alone)
- Internet makes potential victims easily accessible (and plentiful)
- Micro-crime



- Falling for a scam is an *error in judgment*
- It involves a *betrayal of trust*
- *Scammers seek to induce the errors of judgment.*
- Let's look at some methods next ...

MATHEMATICALLY ANNOYING ADVERTISING:

$A \cup B = \{x : x \leq 15 \text{ or } x > 15\} = \mathbb{R}$



← 10 -5 0 5 10 15 20 →
%

WHEN DISCUSSING REAL NUMBERS, IT IS IMPOSSIBLE TO GET MORE VAGUE THAN "UP TO 15% OR MORE."

FREE!

IF SOMEONE HAS PAID \$X TO HAVE THE WORD "FREE" TYPESET FOR YOU AND N OTHER PEOPLE TO READ, THEIR EXPECTED VALUE FOR THE MONEY THAT WILL MOVE FROM YOU TO THEM IS AT LEAST \$ $\frac{X}{N+1}$.



↑ AMOUNT YOU SPEND

NEGATIVE SLOPE

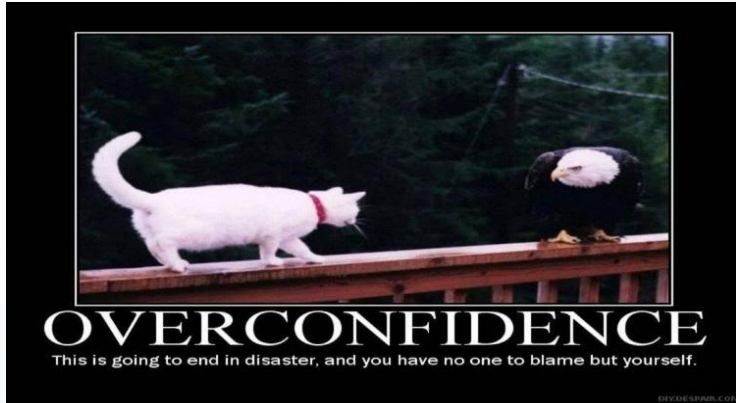
AMOUNT YOU SAVE →

IT WOULD BE DIFFICULT FOR THE PHRASE "THE MORE YOU SPEND THE MORE YOU SAVE" TO BE MORE WRONG

- **Individuals with unfulfilled visceral desires tend to focus on that aspect of themselves - *hungry people think exclusively about food, lonely people about companionship...***
- ***In the context of a scam:***
 - ***Scammers offer many incentives in hopes that one of them fulfils visceral desires (money, companionship, health, job security...)***

- **Self-regulation (or self-control, for the purpose of this presentation) weakens under prolonged exposure to stimuli**
- **In the context of a scam:**
 - Repeated bombardment with scam offers (*sucker lists*).
 - Constant pressure (“*You need to respond now*”)
 - Ties in nicely with *impatience* (i.e. need for instant gratification)

- People tend to comply to requests of authority figures
- e.g. Once potential falsehood of interpersonal communication is hard or impossible to determine, individuals decide mostly on the basis of perceived trustfulness and authority of the other party (Selin, 2006).
- *In the context of a scam:*
 - Fake antivirus companies



- Research has shown, that many victims are overconfident when responding to fraudulent offers.



- *Note that these work in general and in the workplace!*
- **First of all: There is no such thing as a free lunch!**



- **Anyone faced with something that seems too good to be true should ask themselves:**
 - **Why me specifically?**
 - **How likely is this? (include human factors)**
 - **What are the hidden costs?**
 - **What is the *hook*?**

- **Common way to fall for a scam is to read it and respond to it**
 - **Simplest recommendation we can give is to bear in mind previous recommendations and as soon as red flags are raised, delete the email or social post.**

The End