How to obtain passwords of online scammers by using social engineering methods

Andreas Zingerle
University of Art and Design
Linz, Austria
andreas.zingerle@ufg.at

Abstract*—This paper addresses three social engineering techniques that vigilante online communities of scambaiters use for 'Inbox diving': an act of gaining access to internet scammers email accounts. The methods have been gathered by analyzing scambaiting forums and were put on the test in direct email exchange between the author and Internet scammers. By diving into the scammers inboxes, their working methods can be observed, gang structures investigated and potential victims warned. I discuss the moral issues an 'inbox diver' faces and question the ethics of scambaiting communities that prefer social engineering techniques rather than hacking email accounts. The research lead into the creation of the artistic installation 'Password:***' and presents an artistic position dealing with password security.**

***Keywords*-Unsolicited electronic mail, Scambaiting, Interactive fiction, Internet security, social engineering, Vigilante Online Communities.**

I. Introduction

Internet cafès are regularly used by scammers as a working environment for their criminal activities [6], [17]. Besides easy access to office equipment, the scammers can also camouflage their identities and operate anonymously in the mist of other cafè users. Since scammers have to share the equipment with others, most of them store important documents online. The email accounts become their cloud storage where scripted messages, fake documents, harvested addresses, login details or gang communication with further fraudsters are saved. Law enforcement authorities find it particularly hard to catch scammers and thus gaining access to scammers' inboxes can provide valuable insights into their practices.

In April 2014 a major security bug called 'Heartbleed' was detected, allowing anyone to read the servers memory by a vulnerable version of the OpenSSL software. By doing so it was possible for attackers to eavesdrop on various communication, read names and passwords and to impersonate services and users [15]. Netizens were advised to alter all their passwords after the security flaws were patched [18].

Recently yahoo's user-login information was leaked and since people reuse passwords across multiple sites hackers could use them to access other sites [8]. Hacked email accounts are also used to reset passwords to other web services often resulting in identity theft [11]. Often, the password strength is weak and vulnerable to brute force attacks. Two-step authentication is not yet widely used and passwords are seldomly changed so they can be guessed quite easily.

A vigilante subgroup of the scambaiter community illegally enters and observes inboxes of scammers and documents ongoing scam attempts. They use storytelling and social engineering tactics to scam the scammers consequently gaining access to their inboxes [19]. Scambaiters try to get the trust of scammers by posing as a gullible victims with fake characters and compelling storytelling strategies. Scammers and scambaiters use similar social engineering techniques and online tools to persuade the counterpart. This paper, addresses the following issues:

- Bringing forward three case studies where scambaiters use social engineering techniques to gather sensitive data from the scammers (Section II.A, II.B, II.C). Surprisingly, so far only the methods of scammers have been discussed, yet scambaiters use similar tactics to counter fight the scammers.
- Layout moral controversies an 'Inbox diver' faces when analyzing a criminals inbox (Section IV.).
- Artistic positions dealing with online security (Section V.).

II. Social engineering - skillful manipulation of users

Social engineering is defined as a 'hackers use of psychological tricks on legitimate users of a computer system, in order to obtain information he/she needs to gain access to the system' [14] rather than 'breaking into the system' [4]. Through skillful manipulation of the human counterpart hackers avoid the security measurements that companies install to keep a system or a password secure. Similar techniques used by scammers to persuade their marks have been widely discussed [12], [2], [13], [5]. Less attention has been given to cover social engineering techniques of scambaiters.

A. Method 1: Fake Form Elicitation

Scambaiters often use self-made documents to gather additional information about the scammers. During the ongoing fictional narrative baiters claim to need the forms filled out in order to continue the unfolding business preparations. These forms often resemble existing businesses e.g. local bank branches, money transfer companies or forms that

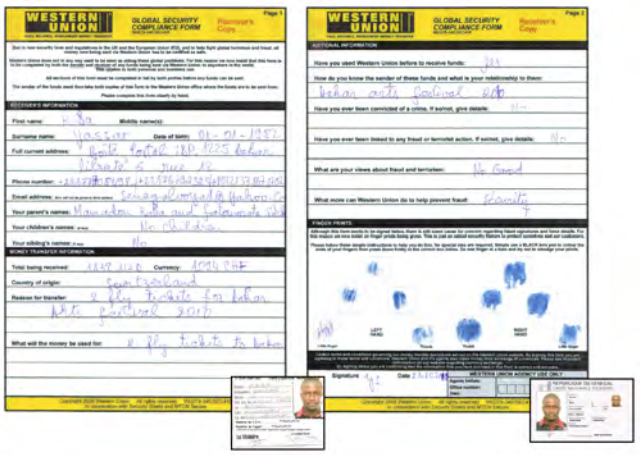

Figure 1. A fake form filled out by a scammer

follow governmental application procedures. Besides asking for personal information like full name, address or phone number they request official documents to validate the scammers identity. Figure 1 shows the fake Western Union 'Global security compliance form'. The fund receiver has to provide detailed personal information and state reasons why the money is transferred. Furthermore the scammer is asked for personal views on fraud and strategies to prevent it. To enhance security fingerprints and official identification cards have to be provided. The documents are shared within the scambaiting community and are considered a 'trophy' when a scammer fills them out and returns them. These questionnaires can include the email security questions which are then used to reset a password and gain access to the scammers email account. With this tactic moral dilemmas can occur because scambaiters don't want to provide the scammers with reusable forms which they can send to real victims.

B. Method 2: Spear-Phishing money transfer

Another attempt is to use a phishing technique where the scambaiter claims to wire all the requested money retrieval information straight to the scammers email account. Through a fake website (see Figure 2) the scammers have to login to their email accounts in order to use the money transfer service. The scammers never collect any money but receive an error message that the service is not applicable in their country, but have already shared the password of the email account with the scambaiter.

Similar to the successful phishing attempts this social engineered tactic lures the scammer to a fake website to disclose sensitive information. Still, this method differs from a phishing attempt since a trustworthy connection between the communicators is already built up through email correspondence. Additionally, a scammer uses the phishing attack for financial gain. Also the scammer has the feeling

Figure 2. A scambaiters phishing website

of superiority since the supposed victim seems to believe the story and is wiring money.

C. Method 3: Phishing web service attack

In the third method a scambaiter offers a supposedly free web service to scammers. It is specifically advertised as 'trusted and reliable infrastructure' that scammers can use for their businesses. The scambaiter sends out email formats of bulk messages in order to attract the interest of scammers to sign up for his service. In one format, he imposes a fellow scammers who shares a good tip to use a reliable bulk emailing service. In order to use the webmail service the scammer has to follow a link to a registration page. During the application process the scammer has to provide several alternative email addresses and a selection of passwords. Scammers who use several fake identities often use same or similar passwords for their Email accounts. Once the scammer logins to the new generated account and tries to use the service for fraudulent activity, it becomes clear evidence that the person tries to scam people and the email and password details are stored in a database. This database is shared amongst the scambaiting community to crowd-source the high amount of scammers account details. Fellow scambaiters can use the scammers login details to dive into their accounts.

III. Access granted - warning victims

Once access to the scammers' inbox is granted there is a suggested procedure to follow while looking through the emails. First, lookout for potential victims who are in

regular contact with the scammer and believe the story of the scammer, or even worse, are ready to pay the money. These victims should be warned and are advised to stop any correspondence with the scammer. Victims who already invested emotionally as well as financially in the scam are seldomly open to accept that they have been fooled. Therefore to gain the trust of the victim, the warners pose as the victims webmailers security officials (e.g. Gmail Security Alert) or as an independent anti-fraud group as in this following example:

> You do not know me, but I am merely trying to help, as you have fallen victim to a dangerous attempt to defraud you of money. The person you have been in contact with [...] operates a so called 'Nigerian 419' type of email fraud. While monitoring his criminal activities, we saw his attempts to victimize you, and that is how we obtained your email address.
> Do not send him any money, but if you already have, then"immediately" attempt to cancel your payment. If you have lost money, contact your local law Enforcement so that they can guide you with the next steps. [...]
> DO NOT CONTINUE TO SPEAK OR WRITE TO THE CRIMINALS WHO ARE RUNNING THIS SCAM.
> Also, PLEASE DO NOT tell the scammer you have been warned, as they will simply open a new Yahoo account and move on before others like you can be warned. Thank you.
> Finally, please - do not feel embarrased or ashamed if you have lost money to this man. YOU ARE NOT ALONE. Countless thousands, possibly millions, of people fall prey to this exact type of scam every year; 419 Fraud is rampant on the Internet.[...]
> Feel free to write us back, if you like, or find out more information about internet crime from the links below. [...]
> Signed, The Coalition to STOP 419 Cybercrime

Once all potential victims are warned the inbox is further scanned for credit card numbers or bank account information. The account details are further reported to bank officials or credit card fraud departments who monitor the accounts. For this the scambaiter forwards a copy of the scammers email including the account holders name, bank name and address, account number, IBAN and BIC code.

Often the scammers are registered to other web services with the same email address or use other email addresses with the same password. By looking through newsletters or notification emails passwords to these accounts can be found or new passwords can be requested. This makes it easy to access other web platforms (e.g. Dating Websites, Social Media) where the scammer creates fake profiles in attempt to scam people.

IV. Moral issues

After the inbox is scanned and collected information reported each scambaiter has to decide how to proceed with the account: Deleting or to continue monitoring it. By closing the webmail account the scammer loses his emails, hooked victims and other gang communications all at once. On the other hand the scammer can easily setup a new account and continue the activities. By monitoring a scammers account it is possible to learn from their activities, constantly warn victims and therefore making all the fraudsters scam-efforts unproductive. Depending on the scammers activity-level, this can be a time consuming task. It can always happen that the scammer and the scambaiter access the mailbox at the same time, creating a very intimate moment for the scambaiter who can then observe in realtime the reading, writing and sending of emails.

Amongst the scambaiting communities there are different moral positions on 'Inbox diving'. Since accessing another persons email account is against the law, forums like 419Eater point out its illegality in their guidelines[1]. Still many scambaiters consider it an efficient way to warn victims and since they access the mailboxes of criminals they don't fear any legal consequences. 'Inbox diving' can be seen as a highly questionable and illegal act - yet it is an effective subcategory of scambaiting.

V. The artwork Password:******

The research on 'Inbox diving' lead to the creation of the artwork called 'Password:******'. The installation consists of a six channel video installation and reveals over 1000 email-passwords used by internet scammers. By scraping a password database (as described in Section II.C) and structuring the entries according to popular words used within the password it unveiled that the words: 'good', 'love', 'money', 'mother', 'jesus' and 'bless' are often used by scammers. This heavily charged words expose personal perspectives of the scammers' and other cultural value systems that seem to be in contradiction to their fraud activities. The passwords are arranged typographically in six stars representing a standard password field for webmail services like Gmail, Yahoo Mail or Outlook (see Figure 3) [16].

Each of the six stars contains of passwords with one of the above mentioned words. The stars are animated

[1]This paragraph is taken from the 419Eater forum: Section 'What is absolutely not allowed': [...] We do not support the sending of viruses and "trojans" to the scammers, nor attempts to hack, phish or hijack their email accounts and/or computers. Viruses and "trojans" will be unknowingly spread to the computers of innocent people and we are only trying to make it difficult for the scammers. On top of that, the spreading of viruses and hacking attempts is an illegal activity in the UK, where this Board is located, as well as many other jurisdictions. Please do not start topics on such subjects. Such threads can and will be deleted on sight.

Figure 3. Photo of the installation setup

shifting slowly in brightness between four layers, always high lightening one of the layers. In the first layer one of the six words is brought to the spectators attention. Thereafter the words and letters are highlighted followed by uppercase letters and numbers (see Figure 4). The animations show that scammers most often use lowercase letters combining two-words and add numbers to it in the end. By looking through the animations the visitor reflects on issues of online security and questions the personal password usage. The artwork stresses on the 'online common sense' that passwords can just be hacked because of security flaws like 'heartbleed' but can also be obtained by social engineering techniques. Securing personal online data with a strong password and constant security updates to avoid exploits is essential. Still each person stays the weakest link when it comes to securing this password and not sharing it with others.

A. Related artistic positions

Recently leaked password lists[2] of web platforms like Linkedin, Yahoo, Youporn or Rockyou have become the new 'cracking dictionaries' for cryptoanalysts and hackers. These lists are often obtained by attacks on computer servers. Using these dictionaries reduces the number of trials that are required to repeatedly guess the correct password to access their e-mail and other online services. [1] Aaram Bartholl published the book series *'Forgot your password?'* where he printed 4.7 million passwords of the leaked Linkedin passwords [10] list in alphabetical order in eight books. Visitors are invited to lookup their password. In another series called *'Private password'* he printed 10.000 Linkedin passwords on dibond plates [3].

In 2014 the Ars Electronica museum hosted the exhibition *'Out of control'* where some of the displayed installations educated visitors about security and cryptography. One of the works is named *'Password hacker station'* [9] created by Jürgen Fuss where visitors had the possibility to enter a

[2]http://thepasswordproject.com/

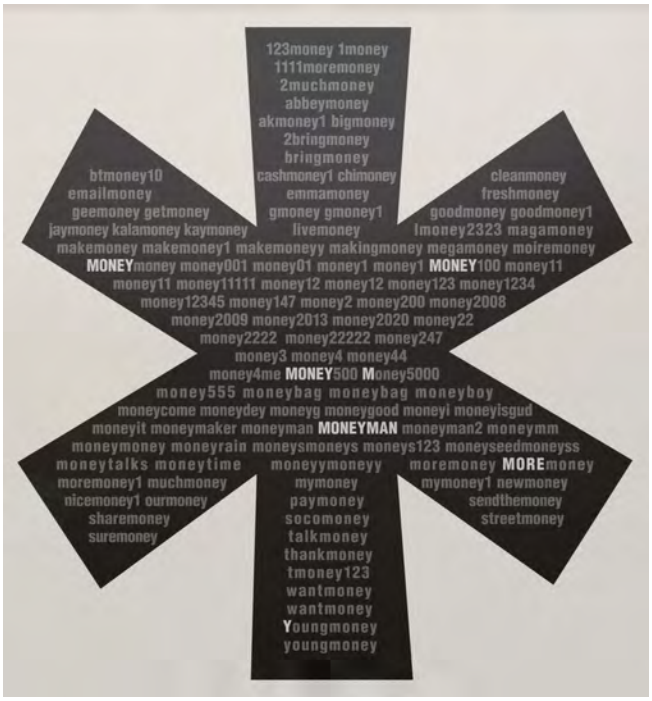

Figure 4. Detailed view of one star

password and analyze how long a standard PC would take to decipher it.

Dana Karwas and Liubo Borissov created the *'Fursicle Safurry'*. The artwork invites people to enter a space of make-belief adventure through the wilderness of telecommunications. First, visitors have to call the fursicle and recap a given password comprised out of animal sounds. Once accepted, the visitor can choose between the features mate, kill or run and further interact with the fursicle and the corresponding sound [7].

VI. Conclusion

Scammers and scambaiters use similar social engineering techniques like 'phishing web service attack', when they are in contact with each other. By collecting information scambaiters receive sensitive data to obtain access to the scammers email accounts. In this paper three social engineering techniques were described and the moral aspect of accessing other people's inboxes were discussed. When access to an inbox is possible, scambaiters look for potential victims that they can warn to stop further payments to the scammer. Within the scambaiting community it is widely discussed how to proceed with a scammers inbox after all victims are warned and other evidence is secured. Part of the research was the development of the artwork 'Password:******' that visualizes scammers behavior to secure the access to sensitive data. It visualizes that people put very little effort into having a strong and secure password showcasing that humans remain the weakest link in any

security system where people can be easily tricked into doing something that undermines their online security. Amongst other related works the artwork encourages visitors to reflect their personal online security strategies and adds the security flaw of 'social engineering' sensitive data to the discussion.

REFERENCES

[1] Anderson, N., *How I became a password cracker*, [Online]. Available: http://www.wired.co.uk/news/archive/2013-03/25/cracking-passwords/page/2, 2013.

[2] Atkins, B., Huang, W., *A Study of Social Engineering in Online Frauds*. Open Journal of Social Sciences, 1, 23, 2013.

[3] Bartoll, A., *Forgot your pasword?*, [Online]. Available: datenform.de/forgot-your-password.html?

[4] Berg, A., *Cracking a Social engineer*, [Online]. LAN Times, Available: http://packetstorm.deceptions.org/docs/social-engineering/socintro.html, Nov. 6, 1995.

[5] Bregant, J., Bregant, R., *Cybercrime and Computer Crime*. The Encyclopedia of Criminology and Criminal Justice, 2014.

[6] Burrell, J., *Invisible Users: Youth in the Internet Cafès of Urban Ghana*. MIT Press, 2012.

[7] Debatty, R., *Fursicle Safurry*, [Online]. Available: http://we-make-money-not-art.com/archives/2005/09/fursicle-safurr.php#.Uzl4gMd4HLe, Sep 22, 2005.

[8] Galbraith, R., *Yahoo says email accounts hacked, passwords stolen*. [Online]. Available: http://www.cbc.ca/news/technology/yahoo-says-email-accounts-hacked-passwords-stolen-1.2518625, Jan 31, 2014.

[9] Fuss, J., Mayrhofer, A., Macala, M., Sojer, M., Vogl, A., *Password Hacking Station*. 'Out of control' exhibition, Ars Electronica Center. 2014.

[10] Perlroth, N., *Lax Security at LinkedIn Is Laid Bare*. [Online]. Available: http://www.nytimes.com/2012/06/11/technology/linkedin-breach-exposes-light-security-even-at-data-companies.html, Jun 10, 2012.

[11] Krebs, B., *The Value of a Hacked Email Account*. [Online]. Available: http://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/, 2013.

[12] Longe, O. B., Mbarika, V., Kourouma, M., Wada, F., Isabalija, R., *Seeing beyond the surface, understanding and tracking fraudulent cyber activities* arXiv preprint arXiv:1001.1993. 2010.

[13] Mann, I., *Hacking the human: social engineering techniques and security countermeasures*. Gower Publishing, Ltd. 2010.

[14] Palumbo, J., *Social engineering: What is it, why is so little said about it and what can be done?*, SANS Institute, [Online]. Available: http://www.sans.org/infosecFAQ/social/social.htm, 2000.

[15] Schneier, B., *Heartbleed*, [Online]. Available: https://www.schneier.com/blog/archives/2014/04/heartbleed.html

[16] Waddilove, R., *Whats best free email service*. [Online]. Available: http://www.pcadvisor.co.uk/features/internet/3448241/whats-best-free-email-service/

[17] Warner, J. *Understanding cyber-crime in Ghana: A view from below*. The International Journal of Cyber Criminology, 5, 736-749. 2011.

[18] Wood, M. *Flaw Calls for Altering Passwords, Experts Say*. [Online] http://www.nytimes.com/2014/04/10/technology/flaw-calls-for-altering-passwords-experts-say.html

[19] Zingerle, A. *Towards a categorization of scambaiting strategies against online advance fee fraud*. The International Journal of Art, Design and Technology. 2014.