

Analyzing Art, Culture, and Design in the Digital Age

Gianluca Mura
Politecnico di Milano University, Italy

A volume in the Advances in Media,
Entertainment, and the Arts (AMEA) Book Series

Information Science
REFERENCE

An Imprint of IGI Global

Managing Director:	Lindsay Johnston
Managing Editor:	Keith Greenberg
Director of Intellectual Property & Contracts:	Jan Travers
Acquisitions Editor:	Kayla Wolfe
Production Editor:	Christina Henning
Development Editor:	Eleana Wehr
Cover Design:	Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: <http://www.igi-global.com>

Copyright © 2015 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher. Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Analyzing art, culture, and design in the digital age / Gianluca Mura, editor.
pages cm

Includes bibliographical references and index.

ISBN 978-1-4666-8679-3 (hardcover) -- ISBN 978-1-4666-8680-9 (ebook) 1. Technology and the arts. 2. Arts and society. 3. Digital media--Social aspects. I. Mura, Gianluca, 1965- editor.

NX180.T4A53 2015

700.1'05--dc23

2015015527

This book is published in the IGI Global book series Advances in Media, Entertainment, and the Arts (AMEA) (ISSN: Pending; eISSN: pending)

British Cataloguing in Publication Data

A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.

Chapter 14

Revealing Passwords: Using Social Engineering Methods to Monitor Scammer Email Communication

Andreas Zingerle
University of Art and Design Linz, Austria

ABSTRACT

*This chapter addresses three social engineering techniques that diligente 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. The author discusses the moral issues an 'Inbox diver' faces and questions 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 the data sculpture 'Monitoring Harry Brooks' and presents two artistic positions dealing with password security and data visualization.*

INTRODUCTION

Scammers regularly use Internet cafés as a working environment for their criminal activities (Burrell, 2012), (Warner, 2011). Besides easy access to office equipment, the scammers can also camouflage their identities and operate anonymously in the mist of other café 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 email addresses, login details to other accounts 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 at-

DOI: 10.4018/978-1-4666-8679-3.ch014

tackers to eavesdrop on various communication, read names and passwords and to impersonate services and users (Schneier, 2014). Netizens were advised to alter all their passwords after the security flaws were patched (Wood, 2014).

Recently LinkedIn's and yahoo's user-login information was leaked and since people reuse passwords across multiple sites hackers could use them to access other sites (Galbraith, 2014), (Perlroth, 2012). Hacked email accounts are also used to reset passwords to other web services often resulting in identity theft (Krebs, 2014). Often, the password strength is weak and vulnerable to brute force attacks. Two-step authentication is not yet widely used and passwords are rarely changed so they can be guessed quite easily.

A subgroup of the scambaiter community enters and observes email 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 (Kronman, Zingerle, 2013). Scambaiters try to get the trust of scammers by posing as 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 chapter, addresses the following issues:

- Bringing forward three case studies where scambaiters use social engineering techniques to gather sensitive data from the scammers.
- 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.
- Two artworks dealing with password security and inbox visualization.

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' (Palumbo, 2014) rather than 'breaking into the system' (Berg, 1995). 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 (Longe, 2010), (Atkins, 2013), (Mann, 2010), (Bregant, 2014). Less attention has been given to cover social engineering techniques of scambaiters.

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 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' and two identity cards that were submitted by a scammer. The fake forms are often used when the scammers asks the counterpart to wire money via Western Union or Moneygram:

Revealing Passwords

Figure 1. A filled out form and identity cards provided by a scammer

The image displays two pages of a Western Union Global Security Compliance Form, along with two identity cards. The forms are filled out with handwritten information in blue ink.

Page 1: Receiver's Copy

RECEIVER'S INFORMATION

First name: Kaba Middle name(s):
Surname name: Vassar Date of birth: 01-01-1982
Full current address: Route Postal BP 1225 Kaba
Libate 5 rue 12
Phone number: +22177084987221766322254102213387493
Email address: you will not be given to third parties: schagelovoyall@kaba.co
Your parent's names: Mamadou Kaba and Fatoumata Sidi
Your children's names: or age: No children
Your sibling's names: or age: No

MONEY TRANSFER INFORMATION

Total being received: 1132 USD Currency: 1094 CHF
Country of origin: Switzerland
Reason for transfer: 2 fly tickets for Kaba
Arts festival 2016
What will the money be used for: 2 fly tickets to Kaba

Page 2: Receiver's Copy

ADDITIONAL INFORMATION

Have you used Western Union before to receive funds: Yes
How do you know the sender of these funds and what is your relationship to them:
Kaban arts festival 2016
Have you ever been convicted of a crime. If so/not, give details: No
Have you ever been linked to any fraud or terrorist action. If so/not, give details: No
What are your views about fraud and terrorism: No Good
What more can Western Union do to help prevent fraud: Security

FINGER PRINTS

Although this form needs to be signed below, there is still some cause for concern regarding false signatures and false details. For this reason we now insist on finger prints being given. This is just an added security feature to protect ourselves and our customers. Please follow these simple instructions to help you do this. No special ink is required. Simply use a BLACK ball pen to colour the ends of your fingers then press down firmly in the correct box below. Do one finger at a time and try not to smudge your prints.

LEFT HAND: Little finger, Thumb, Ring, Middle, Index, Pinky
RIGHT HAND: Little finger, Thumb, Ring, Middle, Index, Pinky

Signature: Yes Date: 2.1.2016

WESTERN UNION AGENCY USE ONLY

Agents details: Office number: Date:

IDENTITY CARDS

The image shows two identity cards. The one on the left is a Western Union Agency Card for a man named Kaba, with a photo and signature. The one on the right is a Senegalese National Identity Card (Carte Nationale d'Identite) for a man named Kaba, with a photo and official stamp.

Dear Ms. Astou,


I just went with our bookkeeper to the local Western Union service agent. There is no online transfer possible to sent money from Switzerland to West Africa. The owner of your Western Union account has to print and fill out the attached form and return it before I can go there again to make the payment. A copy of a passport or official ID will be needed as well. After receiving this forms we can make the payment.

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 that 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 that they can send to real victims. To avoid the reuse of forms, funny address names or number combinations of '419' (to indicate fraud) are included.

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:

Figure 2. A scambaiters phishing website



The Easiest and most Affordable way to transfer funds.

RECEIVE FUNDS | SEND FUNDS | LOGIN / YOUR ACCOUNT | ABOUT US

ACCOUNT HOME | TRANSFER FUND | UPDATE PERSONAL DETAILS | MESSAGES | Log-off

You are logged into account number 082392-4270080

Account Holder: Harold Genetalia
 Account Type: Online Transfer Global
 Account Number: 4270080
 Currency: USD

Account Statement

Payments
 Bill Pay
 Bill Pay View
 Pay Anyone
 Overseas
 Tax
 Periodic
 Pending

Manage...
 Your Accounts
 Your Details

Quick Support
 FAQs
 Handy Hints

Current Balance	\$327,918.43
Funds Available	\$291,206.24

Transaction History		Page	1	of 29
Date	Item Description	Debit	Credit	
26-May-12	International Banking Transfer A43-924-3232 james_6666@yahoo.com Euro 1,200 @ 1.2576	1,509.12		
25-May-12	Inbound Bank Transfer JP Morgan Chase #170424120		250,000.00	
23-May-12	Automatic Bill Pay St. Louis Water and Sewer District	63.45		
24-May-12	International Banking Transfer A23-464-8924 acntspay@toshiba.co.sg	13,842.93		
23-May-12	International Banking Transfer A22-318-4710 rjohnson@gmail.com	2,861.71		
19-May-12	Inbound Bank Transfer United States General Services Administration Homeland Security Invoice 2012-867138		36,712.19	
14-May-12	Automatic Bill Pay Ford Motor Credit Master Lease #80R270Z2	2,355.48		
12-May-12	Automatic Bill Pay Commonwealth Edison Utilities	1,435.78		
10-May-12	Domestic Bank Transfer C67-193-2301 ADP Payroll Services #80972552	126,794.63		

Revealing Passwords

Dear Onyekwe James Peter,

Thank you for using 'Funds Transfer Online', the new fast, efficient and secure method of sending money abroad, that saves up to 70% of the cost of normal carriers.

Our customer [...] has sent you a payment through our system, details below: [...]

You can go to the website and log on with your email address and your password.

After successfully logging in your account you have the possibility to either 1.) Wire the money on your private account using online banking transfer service OR 2.) Receive a MTCN (Money Transfer Control Number)

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

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 scammer who writes in Pidgin English (a simplified version of the English language) and shares a good tip to use a reliable bulk mailing service:

From: Secretary Kofi Annan <koffiannan@XXXXXXXXX.info > Tue, 21 Aug 9:32am

broda i found dis mailer is very good fo bulk i throw more 600 recipient mail go na inbox 100% good u make one too <http://XXXXXXXXX.info>

In order to use the web mail 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 logs in to the new generated account it provides access to a fully functional web mail client that enables them change sender name, reply-to headers, etc. It also gives the look and feel that it is possible to use the webmail service for bulk mailing. As soon as a scammer tries to use the service for fraudulent bulk mailing, it becomes clear evidence that the person tries to scam people. By using several features provided by the mail transfer agent (MTA) every email message coming from one of those web mail accounts is piped through an automated software that will store the message details (like Date, From, Reply-to, Subject and Body text) in the database. Besides saving this evidence

that unmask the web mail user as a scammer, the provided registration details like email address and password along with their name, desired user name, IP address, location and alternative email addresses are added to the 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. The service started in April 2009 and collected over 48000 entries.

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 find it hard to accept that they have been fooled. Therefore to gain the trust of the victim, the activists pose as the victims' web mailers 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 embarrassed 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.

The email accounts are often used to store email scripts, harvested email addresses, fake documents (passport templates, fake identification cards, Anti-terrorism and Drug clearance Certificates) or photos that scammers use as material to tell their stories. These photos and documents get clearly labeled as 'FAKE' or 'used by scammers' and published on anti-fraud websites.

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.

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 real-time the reading, writing and sending of emails.

Amongst the scambaiting communities there are different moral positions on 'Inbox diving'. Since hacking another persons email account is against the law, forums like 419Eater point out its illegality in their guidelines¹. 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 act - yet it is an effective subcategory of scambaiting.

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 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) (Waddilove, 2014).

Figure 3. Photo of the installation setup



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

In West African culture people tend to use their cars as billboards to express their personality and values about life. Religious themed stickers constitute a large majority amongst this car decorations,

Figure 4. Detailed view of one star



Revealing Passwords

among others ‘God is good’, ‘I love Jesus’, ‘Praise the Lord’, ‘Blessing’, ‘God is Great’, ‘No money - No women’, ‘Trust God’. Figure 5 shows one of this car stickers and also one of the many small shops that have similar word combinations as their company names that feature the popular password combinations, making them omnipresent in public space.

THE ARTWORK ‘MONITORING HARRY BROOKS’

Another artwork called ‘Monitoring Harry Brooks’ visualizes 274 email replies that an Internet scammer received during a period of 3 months (92 days). The scammer was chosen according to his explanations on trust issues in his initial email:

[...] I also want you to understand that I do trust you and I expect you to show me the same trust and respect in return since trust is a 2-way street. On the other hand, trust is a relationship of reliance. Trust also means being able to predict what other people will do and what situations will occur.

Figure 5. A shop billboard and a car sticker in Ghana



Trust is both an emotional and logical act. Emotionally, it is where you expose your vulnerabilities to people, but believing they will not take advantage of your openness. Logically, it is where you have assessed the probabilities of gain and loss, calculating expected utility based on hard performance data, and concluded that the person in question will behave in a predictable manner. In practice, trust is a bit of both. I trust you because I have experienced your trustworthiness by merely believing in what I have said, even when you have not seen me, and because I have faith in human nature.

He impersonates an U.S. diplomat who is currently based in Benin, West Africa. He seeks assistance to transport a trunk box of \$3.7 million US Dollars from Benin to the United States. People who would help him in this confidential mission would receive a share of the secured money. As a first fee to get the deal going and some necessary papers signed, he asks for the payment of a processing fee ranging between \$83 - \$183 US Dollars. After replying to his email and the exchange of a couple of more emails a 'spear phishing money transfer' was initiated to receive the password of the email account. Once access was established, potential victims who trusted the scammers' business proposals were warned and advised to discontinue the communication with the scammer.

Then each replied email was analyzed and categorized under the following topics: 'insulting e-mails', 'trusted replies', 'paid money' and 'other' including auto replies. During an Artist in Residence program in Ghana the Inbox was mapped to colorful stones that are traditionally braided into hair extensions. In the installation setup as seen in Figure 6 each braid represents one day, the ones with no stone represent days where no emails were received. Each colored stone symbolizes an email and refers to the categories following the mapping below;

Figure 6. A detailed view of the data sculpture



Revealing Passwords

- Red that stands for fire, blood, anger and aggressiveness is used for the insulting replies.
- Yellow stones that stands for gold and richness are used to symbolize when the victims confirmed a money transaction to the scammer.
- Black stones with yellow dots as a potential to gain money are used for the e-mails where the scammers story is believed and trusted.
- The neutral green and brown stones are used for other emails including autoreplies, indicating that the scammer was actively sending out his business proposals.
- Additionally blue stones represent Sundays and divide each month in weekly sections.

The visualization is inspired by various traditional methods that use braided wool, cloth or hair with interwoven stones, textiles or knots. Some examples of this include Native American tribes who used a string of wool as a timeline and attached colored materials to document personal events. The Inca culture created an own binary language by knotting string devices called ‘quipu’ to record both statistical and narrative information. The data sculpture combines traditional West African hairstyle-braiding techniques with colored stones to contextualize the story world of the scammer.

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 chapter 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, reported and reposted on warning sites. Part of the artistic 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. A data sculpture called ‘Monitoring Harry Brooks’ visualizes the feedback a scammer receives when sending out his fraud attempts. By using a traditional braiding technique the aesthetics of the artwork resembles methods to record narratives or record statistical information. Ongoing research analyses the repository of fake documents and photos that scammers store in their accounts and use to create a trustworthy identity.

REFERENCES

Atkins, B., & Huang, W. (2013). A Study of Social Engineering in Online Frauds. *Open Journal of Social Sciences*, 1(3), 23–32. doi:10.4236/jss.2013.13004

- Berg, A. (1995, November 6). Cracking a Social engineer. *LAN Times*. Available: <http://packetstorm.deceptions.org/docs/social-engineering/socintro.html>
- Bregant, J., & Bregant, R. (2014). *Cybercrime and Computer Crime*. The Encyclopedia of Criminology and Criminal Justice. Academic Press.
- Burrell, J. (2012). *Invisible Users: Youth in the Internet Cafes of Urban Ghana*. MIT Press. doi:10.7551/mitpress/9780262017367.001.0001
- Galbraith, R. (2014, January 31). *Yahoo says email accounts hacked, passwords stolen*. [Online]. Available: <http://www.cbc.ca/news/technology/yahoo-says-email-accounts-hacked-passwords-stolen-1.2518625>
- Fuss, J., Mayrhofer, A., Macala, M., Sojer, M., & Vogl, A. (2014). Password Hacking Station. 'Out of control' exhibition. Ars Electronica Center.
- Perlroth, N. (2012, June 10). *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>
- Krebs, B. (2013). *The Value of a Hacked Email Account*. [Online]. Available: <http://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/>
- Kronman, L., & Zingerle, A. (2013). *Humiliating Entertainment or Social Activism? Analyzing Scambaiting Strategies Against Online Advance Fee Fraud*. Cyberworlds (CW), 2013 International Conference on. IEEE.
- Longe, O. B., Mbarika, V., Kourouma, M., Wada, F., & Isabalija, R. (2010). *Seeing beyond the surface, understanding and tracking fraudulent cyber activities*, arXiv preprint arXiv:1001.1993.
- Mann, I. (2010). *Hacking the human: social engineering techniques and security countermeasures*. Gower Publishing, Ltd.
- Palumbo, J. (2000). *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>
- Schneier, B. (n.d.). *Heartbleed* [Online]. Available: <https://www.schneier.com/blog/archives/2014/04/heartbleed.html>
- Waddilove, R. (n.d.). *Whats best free email service*. [Online]. Available: <http://www.pcadvisor.co.uk/features/internet/3448241/whats-best-free-email-service/>
- McMillan, R. (2012, January 27). *The World's First Computer Password? It Was Useless Tool* [Online]. Available: <http://www.wired.com/wiredenterprise/2012/01/computer-password/>
- Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *The International Journal of Cyber Criminology*, 5, 736–749.
- Wood, M. (n.d.). *Flaw Calls for Altering Passwords, Experts Say*. Retrieved from <http://www.nytimes.com/2014/04/10/technology/flaw-calls-for-altering-passwords-experts-say.html>

ADDITIONAL READING

Atta-Asamoah, A. (2009). Understanding the West African cyber crime process. *African Security Studies*, 18(4), 105–114. doi:10.1080/10246029.2009.9627562

Blythe, M., Petrie, H., & Clark, J. A. *F for fake: four studies on how we fall for phish* (pp. 3469–3478). Presented at the Proceedings of the 2011 annual conference on Human factors in computing systems. 2011. doi:10.1145/1978942.1979459

Brunton, F. (2012). *Spam: a shadow history of the Internet*. MIT Press.

Nakamura, L. (2014). ‘I WILL DO EVERYthing That Am Asked’: Scambaiting, Digital Show-Space, and the Racial Violence of Social Media. *Journal of Visual Culture*, 258–273.

Rogers, M. (2003). The role of criminal profiling in the computer forensics process. *Computers & Security*, 22(4), 292–298. doi:10.1016/S0167-4048(03)00405-X

Viégas, F. B., Golder, S., & Donath, J. Visualizing email content: portraying relationships from conversational histories. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 979-988). ACM. 2006. doi:10.1145/1124772.1124919

KEY TERMS AND DEFINITIONS

Artivism: Is a linguistic blend of the words ‘art’ and ‘activism’. Artivism is often used as an activist practice to push political agendas by using art, but a focus on raising social, environmental and technical awareness is also common.

Brute Force Attack: A brute force attack is a cryptanalytic attack that checks all possible keys or passwords until a correct one is found. This method is very fast for short passwords, whereas for longer passwords methods such as the dictionary attack are used.

Digilantes: Digilantes is a linguistic blend of the words ‘digital’ and ‘vigilantes’ and describes online vigilante communities that undertake actions in the pursuit of self-perceived justice without the knowledge or permission by legal authorities.

Digital Storytelling: Digital storytelling describes the practice of everyday people who use digital tools such as social media, blogs, podcasts, video sharing or email messages to tell their stories.

Nigerian 419 Scam: It became a common term for all advance fee fraud scams that are carried out over the Internet. The number ‘419’ refers to the section of the Nigerian Criminal Code dealing with fraud but is not limited to fraud schemes originating from Nigeria.

Phishing: Is an attempt to get sensible information such as bank details, user name and password combinations, insurance details or credit card numbers for malicious reasons. Phishing is typically carried out in email communication by masquerading a trustworthy company and copying their cooperate identity.

Practice Based Research: Is an investigation undertaken to gain new knowledge by means of practice and the demonstrated outcomes of that practice in form of designs, music, digital media, performances and exhibitions.

Scambaiting: It is an act done by vigilante communities who follow different strategies in order to collect intelligence about an ongoing Internet scam. Often, scambaiters pose as ‘blue-eyed victims’ when communicating with scammers in order to waste the scammers time or resources.

Video Installation: Is a contemporary art form that combines video technology with installation art. Popular formats include monitor work, projection and performance.

ENDNOTES

- 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.