Remain Anonymous, Create Characters and Backup Stories: Online Tools Used in Internet Crime Narratives

Andreas Zingerle

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

Abstract. This research takes a closer look at online tools that anti-scam activists use when in contact with Internet scammers. These tools are used for defining one's online character, for progressing the narrative or maintaining anonymity while uncovering the scammer's identity. The tools are easy to use and, when combined together, they offer powerful methods to narrate stories online. This research draws mostly upon primary sources, like interviews with scambaiters or Internet forums, where scambaiters share their stories and discuss the authenticity of dubious online businesses. The discussed methods and tools are utilized while communicating with scammers. In conclusion, this paper illustrates how these tools can also used in other genres such as digital fiction, investigative journalism and advocacy.

Keywords: 419scam, scambaiting, digital narratives, Internet fiction, Computer mediated communication, online communities.

1 Introduction

Today the Web 2.0 is the stage for people's digital stories and online performances. By constantly updating our social media profiles we create a kind of 'accessible privacy' for others, where we display intimate thoughts, share private photos or make small-talk with colleagues [12, 18]. These social media platforms allow us to cultivate and curate our online personas – both our self-representation and self-preservation. Within these complex social structures, we often trust systems more than individuals. Francis Fukuyama defines 'trust' as 'the expectation that arises within a community of regular, honest and cooperative behavior, based on commonly shared norms, on the part of other members of that community' [8].

Online criminals use these social media platforms to construct and backup their online identities. Hiding behind fake characters and stolen identities, they scour the net for gullible victims. They contact people with business proposals, where the victim has to pay a small amount of money in advance in order to gain huge profits. In order to gain the victim's trust, the fraudsters mimic real companies and backup their stories with fake websites and legitimate phone numbers. It is difficult to take official actions against online advance fee fraud due to the fact that they operate on a global scale and individual cases do not meet the financial threshold for international investigations [1].

A. Mitchell et al. (Eds.): ICIDS 2014, LNCS 8832, pp. 81–90, 2014.

On one hand criminals tend to hide behind fake characters and the anonymity offered by online communication, and on the other hand, they discuss their daily lives and habits openly. Criminal organizations like the 'Knights Templar Cartel' use social media to advertise their activities, strengthen public relations and connect to their Facebook followers [4]. By connecting several social media channels, it is possible to trace back 'when' and 'where' a person was and with 'whom'. These kinds of strategies have also been used by Taliban fighters, who created fake Facebook profiles to get in contact with Australian soldiers stationed in war zones around the globe. By analyzing status updates and geo-tagged photos it was possible to detect troop positions and their movements. Ignorant of the consequences, families and friends of the soldiers unwittingly shared classified information with the enemy [7]. Fake personas or identities are also used by law enforcement to apprehend criminals. Although it is against most social media network policies to create fake profiles, cyber-threat analysts like Robin Sage [21] or police officers all over the country use social media for sting operations [5] to gather intelligence during investigations [11, 19]. Additionally, investigative journalists or advocacy organizations are known to use fake profiles to bring forth some of the more troubling sides of computer mediated communications. This was the case when 'Terre des hommes', an organization advocating Children's Rights, carried out a 'sting operation' with a computer-generated profile of a 10-year old Filipina girl. In law enforcement, a 'sting operation' is a deceptive campaign designed to catch a person committing a crime. Normally a law-enforcement officer or a cooperative ordinary citizen play a role as a potential victim or criminal partner and go along with a suspect's actions to gather evidence of the suspect's criminality. In this case, the computer-generated girl posed on video chat rooms as a 'honeypot', a trap set to detect illegal attempts, to catch online predators. The setup ran over two and a half months and more than a thousand men, willing to pay to see her undress in front of a webcam [6], were caught in the act.

Scambaiters also use different digital storytelling tools to monitor scammers, expose their false narratives and dubious businesses, and warn the online community of their practices. As revealed in previous examples, scammers and scambaiters are not the only ones playing hide and seek online. Yet the diverse online communities of scambaiters have developed and made use of several 'easy-to-use' online tools to support their storyline, create believable characters and to cover their digital tracks to stay anonymous. These scambaiters establish communication with scammers and try to gain their trust to either waste the scammers' time or to document their working practices and methodologies. In one interview a scambaiter explained that through his actions he aims to raise online safety issues and make his friends and family more alert in their use of the Internet [2]. In the documentary 'Wham Bam Thank You Scam', the scammed victim Keith, frustrated by the ineffectiveness of local law enforcement, starts to investigate the scam by himself, gathers vital information about the scammers and travels to their offices in Thailand to meet them. This paper reviews scambaiters' storytelling tools, which have been shared and discussed on the popular forums thescambaiters.com and 419eater.com or the online radio show 'Area419'.

Chapter 2 has been divided into three parts, each one addressing a set of tools that scambaiters use:

- Part 2.1 assesses tools that are used to backup the invented storyline, e.g. faking news reports or using forged forms to collect sensitive data.
- Part 2.2 describes methods that are used to develop an online character; e.g. character generators, social media profiles or VoIP communication.
- Part 2.3 lays out online skill-sets to cover your identity and uncover others' fake characters, e.g. Email IP stripping, message trackers to study the scammers' communication behavior, proxies and anonymity networks.

Online tools are developed and used in a number of ways. Chapter 3 examines the use and application of similar storytelling tools in other practices like digital fiction, investigative journalism and advocacy.

2 Storytelling Tools to Gain the Trust of the Counterpart

Scambaiters follow different methods [23] when contacting scammers and use a variety of techniques to enter '419-fictional narratives' [24]. The documentation of a scam connects the personal with larger public issues [13], such as reporting scammers' methods and warning the public about new scam forms on dedicated web forums or reporting bank account details to bank officials. Anthony 'the Failure' DiSano, - the former initiator of the thescambaiter.com anti-scam forum, once claimed that his site members had contributed information leading to dozens of arrests, most recently involving a 419-ring based in Dubai [14]. As earlier examples have shown both law enforcement personnel as well as vigilante scambaiters have to represent a believable character and stick to a concise story to gather information from the counterpart. Both need to stay safe and in digital anonymity. In order for this to happen, scambaiters use proxy servers, TOR routers, fake characters and corresponding e-mail addresses to create their own stories. With a 'fresh' identity they get in contact with scammers, try to gain their trust and creatively improvise with each email to keep the story going. These digital stories often incorporate stereotypical worldviews of other countries and cultures and are used to record, reveal, analyze and interrogate the counterpart [16]. In order to tell their stories, scambaiters (mis)use various vernacular tools and spread their stories over different media channels online. Once contact with the scammer is established, the stories become interactive, where one has to constantly improvise in order to keep the story going and not loose the scammer's trust. In the following paragraphs, I outline popular tools that are used in this genre -

2.1 Story Backup

Forms: When businesses operate on an international level, administrative barriers can easily get in the way. This is a tactic often used by scammers and scambaiters for their own reasons.

To appear professional and gather sensitive data, scammers use forms that victims have to fill out in order to proceed with the business. The forms are either taken from real companies or they mimic businesses like banks, shipping traders, state institutions. Most famous bogus certificates are the Anti-Drug clearance form, the Anti-Terrorist certificate and the Anti-Money laundering certificate. These certificates are allegedly issued by the United Nations, the International Court of Justice or by the local government in the country where the business takes place. Scammers often use these certificates to request another money transfer.

Scambaiters use forms either to waste the scammers time by making them fill out long documents or to gain more information about their various identities. They collect these forms as proof that the scammers believe the scambaiters stories. The filled out forms are considered a trophy and are shared on online forums. A codex amongst scambaiters states that documents sent to the scammers should not provide them with well-designed material that they can reuse on real victims. A widespread example that nearly everyone can use in their storyline is a supposed document from a money transfer company. As an additional security measure for sending money to West African countries, the receivers have to fill it out and attach other documents to proof their identity. Besides standard personal information about the receiver (name, address, phone number) it also includes questions about the money transfer, what the money will be used for or how international money transfer security can be improved. Some forms ask for detailed bank account information, photographs, handwriting proof in form of signatures, or even fingerprints of the receiver. Once the form is filled out it has to be scanned and sent to the scambaiter and then taken to the money transfer agency in order to be able to receive the money. Scambaiters often hide additional information in the form that exposes the fund collector as a scammer to the transfer agents. When the scammer provides the form to the clerk it can cause additional hassles for the scammer, like the involvement of law enforcement. Most often the forms look similar to money transfer institutions and are named: 'Anti-Fraud form', 'Anti-Money laundry form', 'Gold Import Form' or 'Secure Validation form'. Depending on the narrative, other documents can come into use.

Online Generators: 'Online generators' are programs that can perform a certain task quickly and efficiently. The programs are performed online and do not require in-depth editing or programming skills. Most of these programs offer visual previews to adjust the final outcome in real time. There are various generators, ranging from color-matching profiles to instant-poetry. One example is the 'newspaper-clip generator', which lets you create authentic looking newspaper articles. Once details like the name of the newspaper, date, headline, photo and story text are provided, it generates an image with the look of a scanned newspaper article. This tool can be used to furnish evidence to a narrative and foster trustworthiness. Similar generators are used to create magazine covers, concert tickets, receipts, airline boarding passes or handwritten signatures.

2.2 Support Character Building

Character Creator: Each scam narrative needs actors who engage in wild stories on stereotypical corrupt politicians and large sums of money that one can claim as a next-of-kin. An 'identity creator' lets you create a virtual persona with a few clicks of the mouse. By choosing parameters like gender, age, name set and country it is possible to create quite an accurate fake identity. It also provides random street addresses and background information like birth date, occupation, blood type, weight and height. These basic traits help to lend authenticity once the characters' personality, physical appearance or soft skills are further defined. Similar and more advanced avatar creators are well known from computer games e.g. World of Warcraft. During the gameplay according to the users interactions the chosen character is further specialized ('leveled up') in a certain skillset.

VoIP: The 'Voice-over-Internet Protocol' (VoIP) enables the transfer of voice communication and other multimedia communications (voice-messaging, fax, SMS, video) over IP networks. There are several VoIP programs, some are even incorporated in webmail services like 'Google Talk', 'Yahoo Messenger' or 'Outlook's integration of Skype. Scammers are increasingly using these services to be in more direct contact with their marks.

Scambaiters use software to record these calls and share them amongst each other. When assuming the role of a fake character, they use voice-morphing plugins for VoIP programs to pitch their voices, imitating a different gender or someone of a different age. Similar plugins exist for webcam software, where one can edit the video chat in real time and flip through prerecorded files to demonstrate different gestures.

There are also platforms that provide one with call-forwarding numbers, also known as 'global redirects'. That way you get a virtual phone number of your chosen country and whoever calls that number will get routed through to your cell phone number. This is a powerful tool to deceive others of your actual location.

A similar tool provides free voicemail and fax message services. It is possible to personalize one's mailbox message so that it fits to any identity. When someone leaves a voice message or sends a fax, it will be forwarded as a digital file to the provided email account.

In this example the scammer claims to be a businessman from the UK and provides a UK phone number as a form to contact him:

```
Dear Sir, […] I find it pleasurable to offer you my part-
nership in business, for which purpose I have tried to
call your telephone number several times but it seems
disconnected or changed, I only pray at this time that
your address is still valid. […] I look forward to your
response and our partnership, you can call me with this
number + 44 7087624521 anytime.
Regards, Arthur Roy.
```

Tracing the origin of the email reveals that the sender is actually based in Lagos, Nigeria. The phone number is blacklisted as a scammer's phone that uses a call-forwarding service.

2.3 Cover and Uncover

Email IP Stripping: Both scammers and scambaiters use popular email services to create their fake characters. Nowadays these free webmailers include other services like instant messaging, implementation of social media contacts or cloud storage. Depending on the user's needs, these features can be personalized by plugins to show the receivers' social media platforms or delay the sending of the message [20]. A basic feature that scambaiters use is analyzing the email header of the received message. By scanning the header of the message, information like originating IP-address, hostname, country of origin, used protocols and used X-mailing software can be detected (see Fig. 1.). This can provide vital information about the sender's origin. Anonymous webmail services like Tormail are seldom used due to unpopularity and security issues [15].

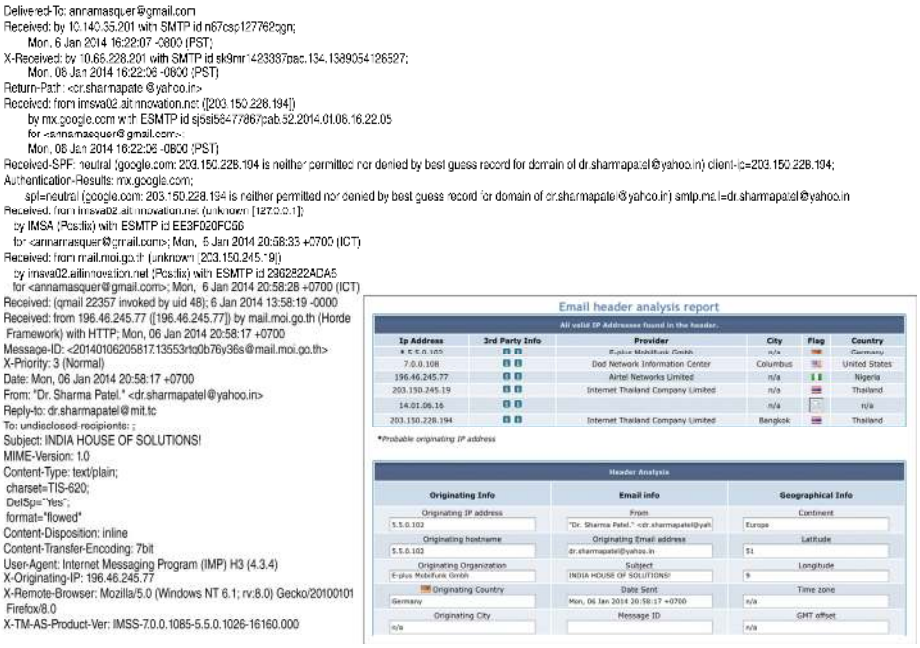

Fig. 1. IP-Header text and screenshot of the online tracking program

Email Trackers: This is another important tool widely used by online marketers to track the email delivery process and study consumer behavior. The tool embeds a tiny, invisible tracking image (e.g. a single-pixel gif) that activates a notification once it has been opened. Similar notifications are sent when the email gets deleted, printed

or forwarded to a different email address. Email trackers normally work on most web-based email services, although there is no 100% guarantee.

A third tool is to use fake mailers as a narrative instrument. A fake mailer enables one to send an email by faking the recipient's email address. This way, it is possible to contact scammers and either play the role of a gang member or persuade the scammer that their inbox got hacked.

Image Analyzers: Scammers often send images to prove their authenticity to their victims. Images that come in the .jpg or .tiff format carry metadata that is stored as 'Exchangeable image file format' data (short Exif-data). When taking a photo, metadata like date, time, camera settings (e.g. camera model, aperture, shutter speed, focal length, metering mode, ISO speed), GPS location information and a thumbnail of the image is saved and embedded within the image file itself. This is mostly done by default without the camera owner's knowledge. This Exif-data is also saved in .wav-audio files.

Scambaiters can analyze the Exif-data and see whether a photo has been edited or where and when it was taken. This can often help to prove the authenticity of a story. According to leaked documents by whistleblower Edward Snowden, the NSA also analyzes Exif information under a program called 'XKeyscore' [9].

In Dec. 2012, when John McAffee was on the run after suspected murder charge, he was interviewed by reporters from Vice magazine in Guatemala. As proof that the reporters were actually with John, they published a photo, which included the Exif-data GPS-coordinates. This revealed McAffee's location to the police who arrested him two days later [22].

Another way to put the authenticity of an image to test is to use 'reverse image search' engines, which specifically search for matching images rather than finding content according to keywords, metadata or watermarks. When an image is submitted, a digital fingerprint is created that gets compared to every other indexed image. The different engines and plugins vary in their accuracy in finding exact matches to similar images, including those that have been cropped, modified or resized.

Websites Archives and Metadata: When fraudsters want to appear more professional and gain the victims' trust they register top-level domains and create fake websites to promote their dubious businesses, e.g. international banks, shipping and logistic companies, rental organizations, law firms or factories. Scambaiters try to uncover these fake websites by searching DNS-database entries for domain setup dates, registration expiration dates, or tracking down the administrator or registrant of a domain name through publicly available (non privacy-protected) directories. They use website archives to trace back the website's history, which is recorded in form of snapshots. These snapshots can serve as evidence when a given website was accessible to the public.

JavaScript Injections: JavaScript is one of the main programming languages of the Web. By using JavaScript code in the browser window, it is possible to access browser cookies, change form input tags and website preferences or perform other real-time

actions like temporary website editing, locating Cross-site scripting (XSS) vulnerabilities and performing malicious operations. The changes one can perform with JavaScript injections are not permanent and won't affect any server information.

An example of a JavaScript injection illustrates how it can be used in storytelling when communicating with scammers. For this, the user types a code snippet in the browser's address bar that makes the content of the page editable. Once the text is changed, a screenshot of the website is taken and used in the upcoming email conversation as evidence. This way, every website can be easily manipulated and no complicated graphic editing software is needed to edit a message into a website.

3 Tools Used in Other Narratives

The tools referred to in this paper as well as similar easy-to-use tools and tactics, can be utilized in other areas of digital storytelling, e.g. tactical activism, investigative journalism or Transmedia activism. Through the use of vernacular media tools character's believability can be reinforced. The following three examples illustrate how diversely these tools and tactics can be (mis)used.

Between 2009 and 2011 an Austrian Neo-Nazi group invoked a witch-hunt for Austrian politicians and NGO workers on their website 'alpen-donau.info'. The website was hosted on US-servers making it impossible to uncover the administrators' identities. The Austrian Data Forensic Scientist Uwe Sailer impersonated a young right wing group 'Tirol1809' and setup a 'canary trap' by sending marked images to a circle of right-wing politicians. A canary trap is a method for exposing an information leak by giving different versions of a sensitive document to several suspects and observing which version gets leaked. The images were scans from a local newspaper where an additional code was embedded in the Exif-data to detect the images once they appear on the website. By doing so it was possible to prove the ties of a right wing politician to the administrators of the illegal website [3].

Investigative journalism programs like 'Exposing the Invisible' by the Tactical Technology collective collect the tools that journalists use in their investigations. Through trainings like 'Privacy and Expression', people learn how to use these tools for their own purpose.

Fognews.ru is a Russian news satire website that publishes fake news of Russian life. It comments on real and fictional events and parodies traditional news websites. On their website they warn their readers with the Latin quote 'Novae res a nobis confictae', meaning 'new things we have made up'. On a number of occasions the published news gone viral and none of the inadvertent participants have had a chance to clarify the situation. For example, on Aug 5, 2012, Fognews reported that the famous pro-Putin conductor Valery Gergiev interrupted a performance of 'Carmen' in London's Covent Garden to give a speech in support of the jailed punk group Pussy Riot. This speech went viral and Valery Gergiev, despite repeated attempts to deny the story, but got very little attention [10].

4 Conclusion

This study has shown that scambaiters use vernacular online tools to create virtual characters and tell stories. These fake personas are used to hide their real identities and to remain anonymous, and also to avoid being prosecuted by the scammers once they find out that they have been tricked. Scambaiters play with these tools to see how easy it is to create a believable online character. Some of the tools are used to examine information received from the scammers. This is used either to validate or negate scammers' stories or to possibly identify the scammers. In this paper these tools are divided into three categories. The tools described in the categories 'story backup' and 'support character building' are used for defining the character and telling the story. Whereas tools outlined in the category 'cover & uncover' enhance media competence skills in both staying anonymous online and proving the authenticity of others. Scambaiters publish their findings on online platforms to expose the working practices of scammers and to warn others. As demonstrated in a number of examples, the discussed tools and tactics can also be used in other avenues – from investigative journalism to transmedia storytelling and online activism.

References

1. Advance fee fraud coalition AFF, http://affcoalition.org/
2. Channel 4, Secrets of the Scammers (January 2, 2014), http://youtu.be/KoTNuZmF_ws
3. Cms, Simo, Post an Neonazis: FP-Politiker unter Verdacht, (March 8, 2011), http://derstandard.at/1297819867094/Post-an-Neonazis-FP-Politiker-unter-Verdacht
4. Cox, J.: Mexico's drug cartels love Social Media (November 4, 2013), http://www.vice.com/en_uk/read/mexicos-drug-cartels-are-using-the-internet-to-get-up-to-mischief
5. Crates, J.: ATF and D.C. Police Impersonate Rap Label; Arrest 70 in Year Long Guns and Drug Sting (December 19, 2011), http://allhiphop.com/2011/12/19/atf-and-d-c-police-impersonate-rap-label-arrest-70-in-year-long-guns-and-drug-sting/
6. Crawford, A.: Computer-generated 'Sweetie' catches online predators (November 5, 2013), http://www.bbc.co.uk/news/uk-24818769
7. Deceglie, A., Robertson, K.: Taliban using Facebook to lure Aussie soldier (Sepember 9, 2012), http://www.dailytelegraph.com.au/taliban-using-facebook-to-lure-aussie-soldier/story-e6freuy9-1226468094586
8. Fukuyama, F.: Trust: The social virtues and the creation of prosperity, pp. 61–67. Free Press, New York (1995)
9. Greenwald, G.: XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. The Guardian (2013)
10. Hoeller, H.: Threatening fake news. Springerin (2012), http://www.springerin.at/dyn/hefttext.phptextid=2695&lang=en

11. Maher, J.: Police create fake Facebook profiles to bust criminals (September 6, 2012), http://archive.news10.net/news/world/208252/5/Police-using-controversial-social-media-tactic-to-bust-criminals
12. Pearson, E.: All the World Wide Webs a stage: The performance of identity in online social networks. First Monday14(3) (March 2, 2009), http://firstmonday.org/ojs/index.php/fm/article/view/2162/2127
13. Lambert, J.: Digital Storytelling. Capturing Lives, Creating Community. Digital Diner Press, Berkeley
14. Milestone, K.: Catching rats - Sporting scambaiters turntables on foreign scammers (April 3, 2007), http://articles.chicagotribune.com/2007-04-03/features/0704030230_1_scammers-con-artists-fraud-center/2
15. Poulsen, K.: If You Used This Secure Webmail Site, the FBI Has Your Inbox (January 27, 2014), http://www.wired.com/threatlevel/2014/01/tormail/
16. Renov, M. (ed.): Theorizing Documentary. Routledge, New York (1993)
17. Schneier, B.: Liars and outliers: enabling the trust that society needs to thrive. John Wiley & Sons (2012)
18. Stoate, R.: Internet Detectives: Performativity and Policing Authenticity on the Internet (2007), http://dichtung-digital.de/2007/Stoate/stoate.htm
19. Kelly, H.: Police embrace social media as crime-fighting tool (August 30, 2012), http://edition.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/
20. Waddilove, R.: What's the best free email service? We compare the top 6 providers (March 10, 2014), http://www.pcadvisor.co.uk/features/internet/3448241/whats-the-best-free-email-service/?pn=1
21. Waterman, S.: Fictitious femme fatale fooled cybersecurity (July 18, 2010), http://www.washingtontimes.com/news/2010/jul/18/fictitious-femme-fatale-fooled-cybersecurity/
22. Wilhelm, A.: Vice leaves metadata in photo of John McAfee, pin-pointing him to a location in Guatemala, Thenextweb Online Insider (December 3, 2012), http://thenextweb.com/insider/2012/12/03/vice-leaves-metadata-in-photo-of-john-mcafee-pinpointing-him-to-a-location-in-guatemala/2012/!zX5oN
23. Zingerle, A.: Towards a characterization of scambaiting techniques. International Journal of Art, Culture and Design Technologies (IJACDT), IGI-Global, doi:10.4018/IJACDT
24. Zingerle, A.: The Art of Trickery: Methods to establish first contact in Internet scams. In: xCoAx Conference, Porto, Portugal (June 26, 2014)