The Unseemly Side of the Internet

Anti-Social Media – Money Mules, Agents, and Dupes

The usual disclaimer

- I don’t know nuttin’ about nuttin’
- All sources are publically available.
- My employer had nuttin’ to do with this presentation. Honest.

Is social media safe?

In a word, no.

With more emphasis on social media for a variety of business uses, users will have to become more sophisticated in spotting social media **chimeras** (false identities).

Chimeras offer something targeted to a user's needs that when viewed critically is too good to be true.

Users should be educated that they personally are being targeted by chimeras for something of value, either money or information.

Users will have to spot chimeras from tell-tale clues in email and in postings to Internet sites.

Social media chimeras

- Facebook has released statistics showing that it believes there are more than 83 million chimeras (false profiles) on its social network.
- Some 8.7% of the site's 955 million user profiles s are believed to be bogus, according to documents that the company filed with the Securities and Exchange Commission (SEC) this summer.
- Co-founder of Reddit, Steve Huffman, admitted that in its early days the site used hundreds of chimeras to post high quality content and thus set the tone for the web site.

Chimera telltales

- Too good to be true – chimera has supermodel looks
- Very large age difference
- Chimera wants to lure you out of web site’s messaging service
- Email address – name and email address do not match
- Email address is script generated and difficult to read.
- Email content is generic and may contain URLs either to malware or affiliate web sites.
- Questions from previous messages unanswered.
- Language syntax and spellings may be strange because of online translators used to craft the message.

Chimeras and dating sites

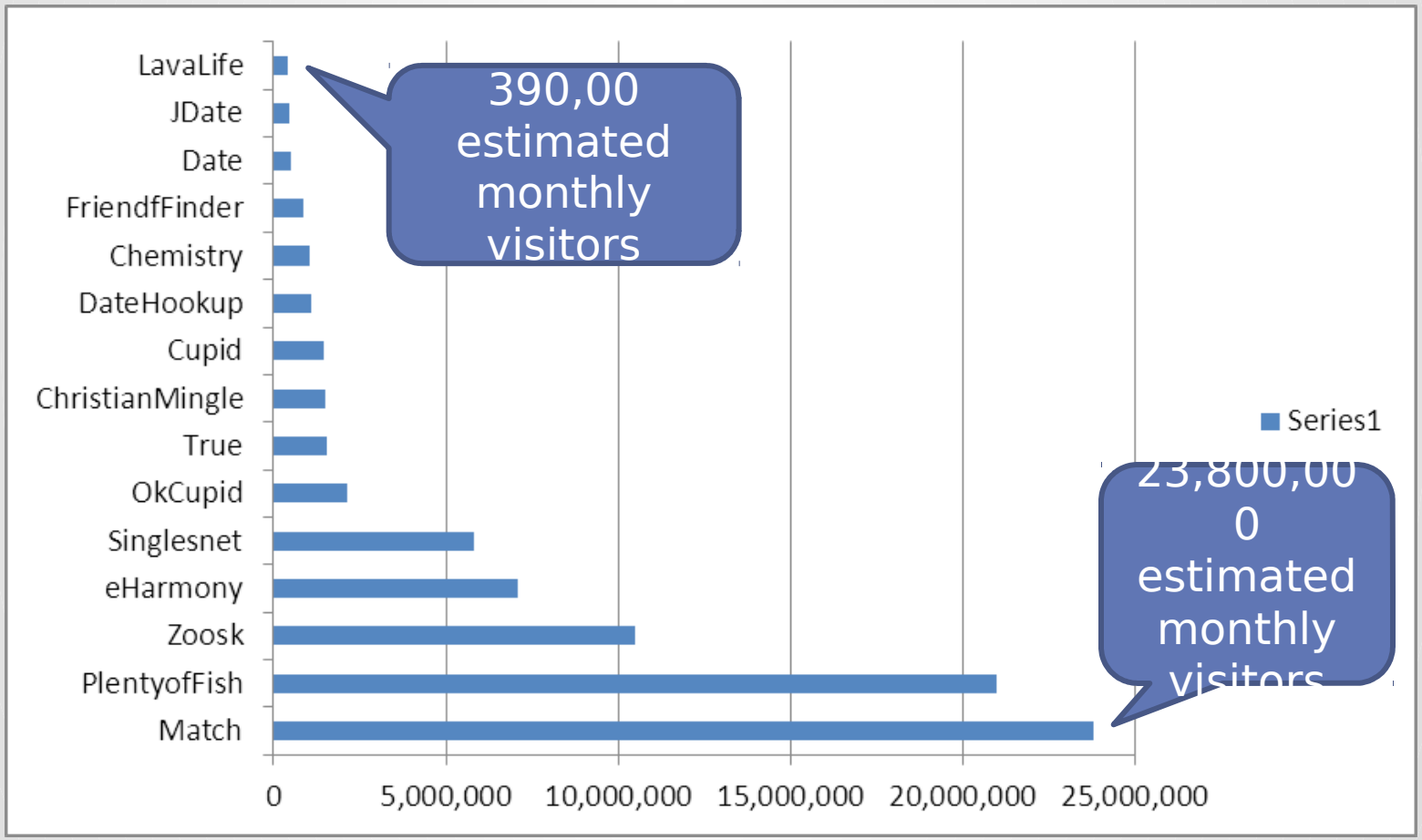
- Some dating sites use chimeras to pad the site with attractive profiles.
- Some site-run chimeras may appear to respond to user interaction as a form of “entertainment.”
- Dating site chimeras may be users with malicious intent.
- Other chimeras may be users just trying to hide their identity.

Read the EULA!

A new adult dating site EULA claims users for the site should have:

- no expectation of privacy;
- no expectation that personal data will be protected;
- no expectation that other site profiles will actually be real;
- no expectation that users will be protected from malicious individuals.

Most popular dating websites Updated 9/10/2012 source: BizMBA



Mobile dating

- Internet dating consultant firm Courtland Brooks says:
- “In 2012 mobile dating is now overtaking online dating. Match.com and POF.com and Badoo now see over 40% of their log-ins coming from mobile phones and mobile dating is expected to generate $1.4 Billion in revenue in 2013 worldwide.”

The players

Dating site affiliates, 419 players

Affiliate scammers

- Affiliate scammers attempt to lure users from web site to dating site where they will receive a commission should the users join the site in order to view the scammers' photos.
- Dating sites realize that this form of deception is counterproductive to long term profits, so they will usually sever relations with the rogue affiliate if exposed.
- This is common occurrence throughout dating sites and personals sites such as Craig's List.
- Most sites warn of scammers. Security response by web sites varies.

Scammers and money mules

- Money mules are persons who often unwittingly transfer funds from criminal activities to overseas accounts.
- They are frequently recruited at online job sites for work-at-home schemes.
- Fraudsters also use dating sites to recruit romantic interests for money mule schemes, often through innocent-sounding ploys such as wiring money overseas to pay for plane ticket or to help a sick relative.

419 Scams

- Nigerian con game, working Westerners, named after section 419 of the Nigerian criminal code.
- Now has other players, notably from Eastern Europe.
- Traditional scam involved money laundering, going back to the early 1800s (the Spanish Prisoner).
- Extended to plane fare, love relationships, sick relative scams.
- Used to be surface mail based, then fax-based, then email.
- Now extended to social networks and many dating services.
- Note: FBI and Secret Service web sites have good info.

Yahoo Boys at work – Source Daily Times of Nigeria

Far from being high-tech operatives, Yahoo Boys are masters at understanding the psychology of their marks.

419 chimera success

- Difficult to measure as folks are not inclined to admit they’ve been taken.
- Australian police figures show Yahoo Boys have conned West Australians of more than $6.5 million since May 2012 to September 2012. That’s more than $1.5 million a month for the past four months. - Sept. 22,2012 *The West Australian*
- U. S. mother and daughter accused of working with Yahoo boys by posing as military members in Afghanistan and bilking victims out of over $1 million. They also wired a portion to Nigerian criminals.

Financial cost of dating scams

- The MoneyGram Corporation reported that through the month of November 2011 they refunded 4,870 transactions, or about $13.7 million in thwarted romance scams.
- National White Collar Crime Center say nationally $485 million lost to Internet Crimes.

Yahoo Boy convicted

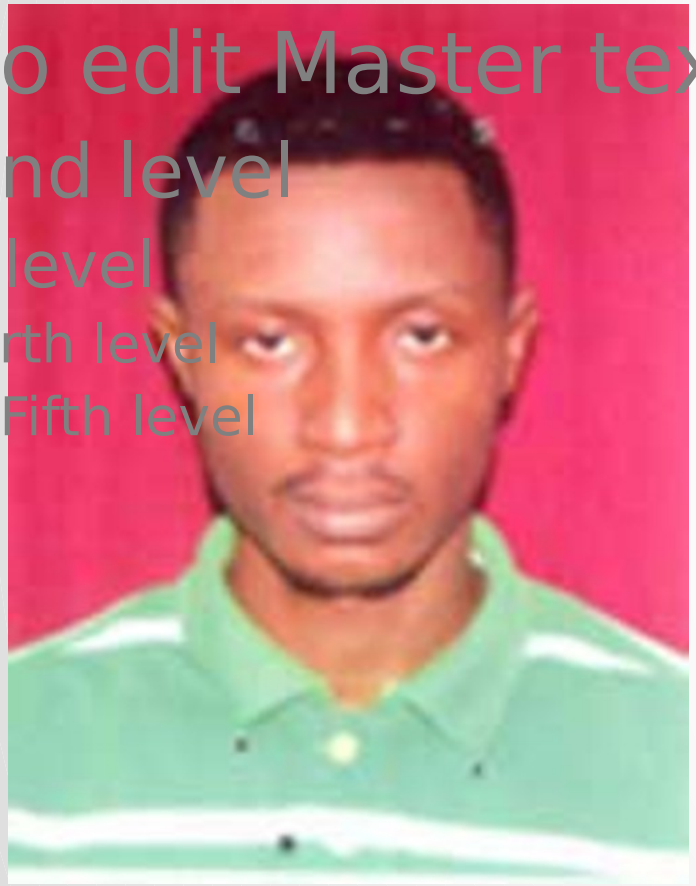
Technology Times Online (Nigeria)

ck to edit Master text styles

Second level

Third level

- Fourth level
  - Fifth level



Bike John Niye – Photo credit EFCC of Nigeria

"Lagos. September 10, 2012: The Economic and Financial Crimes Commission (EFCC) says that 22-year old internet fraudster, Bike John Niye is to spend one and half years in prison for defrauding one Laura Wallmam of Indiana, USA of the sum of $53,500 in an online romance scam."

Nive used online dating service Badoo for scam.

419 Modis Operandi

- For-pay online dating services usually start around $30 a month. Yahoo Boys use stolen credit cards to pay for accounts, thus appearing to be legitimate users.
- Photos and videos may either be stolen from other online dating sites or models may be commissioned for photos and sex videos.
- Yahoo Boys look at the long term.
- They may even send expensive presents in the hopes of bigger payoffs later.
- One even helped his mark find a better paying job.

419 Modus Operandi

- Nigerian con-men known as “Yahoo Boys”
- Serve as emotional prostitutes to Westerners. Yahoo Boy pose as men or women.
- Yahoo Boys work multiple marks, both men and women.
- One Yahoo Boy says in order to con his male marks, he thinks of them as women.
- Yahoo Boys work to establish emotional dependency, even helping marks pick out clothes in the morning.
- Some marks return to handler when scam is blown.

Chimeras as spies

The Robin Sage Experiment

Getting in Bed with Robin Sage

- Provide Security created a bogus persona called Robin Sage who claimed to be a security expert. Using Robin Sage Provide Security befriended intelligence targets.
- During Dec. 2009 – Jan 2010 Sage was offered consulting work with Google and Lockheed Martin. She was invited to dinner by several online male friends.
- “The worst compromises of operational security I had were troops discussing their locations and what time helicopters were taking off,” Provide Security CEO Thomas Ryan said.

Robin Sage aftermath

- Ryan told about the Robin Sage experiment at the 2010 Black Hat conference. He said that his findings could have damaged national security had a terrorist organization used the same tactics.

Technical threats

Technical means that could be used to target marks

Internet repo men

News item – rent to own laptops secretly photographed users having sex, FTC Says

Rent-to-own companies often put and back door software on computers without renters' knowledge so they can recover them should the renters default on payments. This software can turn on webcams and mikes.

http://www.wired.com/threatlevel/2012/09/laptop-rental-/

Supply Side Threat

- On September 13, Microsoft has filed against electronics manufacturers who may have been compromised on the supply side.
- The MS Digital Crimes Unit reported that it purchased 20 new computers manufactured in China.
- Four of these computers contained malware with one linked to the Nitrol Gang.
- http://blogs.technet.com/b/microsoft_blog/archive/2012/09/1

Mobile malware capabilities

- Kevin McNamee, security architect and director at Kindsight Security Labs, says developing Android malware to harvest information is a "trivial" task and possible using readily available tools. McNamee has demonstrated how to inject malware code into a legitimate Android app.
- The malware, when executed, connected with a remote command-and-control center and transmitted data from the device.
- *[Security Week September 27, 2012]*

Cautionary tales

The Taliban, dating dangers, mayhem, and conduct unbecoming.

Taliban chimeras

- The Australian Department of Defense warned that the Taliban was using Facebook profiles to gain information from unsuspecting Australian soldiers.

Online Dating Dangers

- Man using dating app Skout met online friend only to be assaulted and robbed.
- Skout, a location-based dating app, suspended access to teenage users in June 2012 after a series of reported rapes of underage users in the United States.
- British coroner May 2, 2012 revealed two years prior Intelligence cryptographic specialist Gareth Williams was killed at his London home either by poison or suffocation. Examination of his computer revealed hits for bondage, claustrophillia, and sado masochism web sites. Coroner played down this Internet usage.

Murder and Malware

- Journalists and free press organizations are targeted by Trojan horse in spear phishing email.
- Committee to Protect Journalists Advocacy Coordinator Danny O’Brien targeted by phishing attack. C & C server traced to Indonesia. Some code in Chinese.
- No smoking gun that nation-states were involved.
- Articles discuss freelance journalist’s death in Syria.

Conduct Unbecoming

- Navy Commander Michael Ward II dismissed as captain of nuclear submarine USS Pittsburg one week after taking command.
- The Navy said in a statement that Ward was relieved of his duties "due to lack of confidence in Ward's ability to command based upon allegations of personal misconduct on the part of Ward."

Conduct Unbecoming

- Ward had eight month affair with 23-year-old woman he had met online. Affair was exposed by the woman's relative after she had a miscarriage.
- When faced with a transfer to another base, Ward faked his own death using a chimera posing as a coworker to break the news to his lover.
- Ward was charged with dereliction of duty, conduct unbecoming of an officer and a gentleman, and adultery.

Recommendations

What to do

Recommendations

- Don’t share detailed travel plans on social networks, and don’t post pictures and updates from overseas.
- Check your security settings and sharing status on networks, so that only very trusted people can see your details and comment on your posts.
- For smart phones, determine how geo positioning is used within apps and turn off.
- Don’t connect with strangers without thoroughly assessing whether you actually want to or should be associated with them.
- If you’re going to meet someone for the first time that you met online, don’t do it alone and make sure it is in a public place with people around.

References

Web sites consulted for this presentation

References

- Courtland Brooks - http://internetdating.typepad.com/courtland_brooks/
- Online Personals - http://www.onlinepersonalswatch.com/news/2012/09/us-onli
- Mobile dating - http://internetdating.typepad.com/courtland_brooks/2
html

- Fighting scammers:
- http://romancescam.org
- http://www.lookstoogoodtobetrue.com/
- **http://www.ic3.gov/default.aspx**
- **http://www.fbi.gov/scams-safety/fraud**
- http://www.romancescam.com/album/thumbnails.php
- http://www.stop-scammers.com/warning_signs.asp

References

- Psychology of dating dependence:
- http://www.msnbc.msn.com/id/8704213/ns/technology

- Navy relieves sub commander:
- http://abcnews.go.com/US/submarine-commander-faked-dea

References

- Social media dangers:
- http://fearlessweb.trendmicro.com/2012/friends-and-family
- http://www.smh.com.au/technology/technology-news/dating
- http://bits.blogs.nytimes.com/2012/06/12/after-rapes-i/

References

- Supply Side malware threat:
- http://www.infoworld.com/d/security/brand-new-hardw
- http://blogs.technet.com/b/microsoft_blog/archive/201
- Rental equipment comes with spyware:
- http://www.wired.com/threatlevel/2012/09/laptop-rent

References

- Gareth Williams murder: http://www.standard.co.uk/news/crime/profile-mi6-spy-garet
- http://www.huffingtonpost.co.uk/2012/04/23/spy-in-a-bag-mi
- Threat to Journalists:
- http://www.zdnet.com/malicious-malware-targets-journ/
- http://nakedsecurity.sophos.com/2012/09/05/free-pres

References

- Taliban chimeras target Australian forces:
- https://www.commonwealthcu.org/?Cabinet=MAIN&Dr
- http://www.dailytelegraph.com.au/news/taliban-using-
- http://www.defence.gov.au/pathwaytochange/docs/soc

References

- Social media chimeras:
- http://nakedsecurity.sophos.com/2012/08/02/fake-faceboo
- http://www.dailydot.com/business/steve-huffman-built
- The Robin Sage Experiment:
- http://www.robinsageexperiment.com/
- http://science.dodlive.mil/2010/07/21/the-dangers-of-f/

References

- Yahoo Boys:
- http://techcrunch.com/2011/05/15/the-chilling-story-of-genius-in-a-land-of-chro
- http://au.news.yahoo.com/thewest/a/-/breaking/14919785/6-5m-lost-to-online-s/
- http://www.newscientist.com/blogs/onepercent/2012/02/meet-the-yahoo-bo
- http://www.huffingtonpost.com/2012/06/21/tracy-and-karen-vasseur-online-datin
- http://madtainment.blogspot.com/2010/07/center-of-yahoo-yahoo-is-lagos.html
- http://www.technologytimesng.com/news/2012/09/internet-fraudster-jailed-/
- http://www.hutchnews.com/Bizag/19BIZ-BBBcolumn--1