SOCIAL MEDIA DECEPTION

Aamir Lakhani @aamirlakhani
World Wide Technology

Joseph Muniz
Cisco System
Contact Information

► Aamir Lakhani – aka Dr. Chaos
  ► Blog: www.DrChaos.com
  ► Twitter: @aamirlakhani
  ► Senior Counter Intelligence and Cyber Defense specialist

► Joseph Muniz – aka The Security Blogger
  ► Senior Cyber Defense Solutions Architect

► Presentation on our blogs: Search for RSA Europe
Have You Ever Told A Lie?

► People believe white lies are ok
► A Lie Online is like a job application – your taking out the rough edges
► Confidence issues
► It’s better to be forgiven than to ask for permission
► Happens and is expected on most dating websites, job applications, and others.
Your looking at this
What you get is... something better!
Real Penetration Assignment

► Asked to obtain sensitive and confidential information from an organization in an approved penetration tests.
► We were lazy and not very good at programming.
► We thought very least we could have fun and maybe embarrass some people.
► We wanted to avoid Pizza 😊
Warning!

This talk focuses on Facebook & LinkedIn as a method to launch sophisticated attacks however these are not the only Social Engineering attack vectors!

- Creating a fake person
- Social Engineering on Facebook and LinkedIn
- Launch attacks from Social Media sources
- Lessons Learned
Who Are Your Cyber Friends
Josephine ???
The Facts

► 1 in 5 Couples meet online.
► 1 in 5 also blame divorce on Facebook
► 65% of US college students would rather give up sex than the Internet

► Facebook passed Google - most visited internet site.
  • 11% of world’s population has Facebook account.
  • More Facebook accounts than automobiles.
  • If Facebook were a country, it would be the 3rd largest in the world
Robin Sage

▶ **Fictional** American cyber threat analyst created to abstract sensitive information. She graduated from MIT and had 10 years of experience despite she was 25 years old.

▶ Despite her fake profile, she was offered consulting work with notable companies such as Google and Lockheed Marti. She had friends in the FBI, CIA and even offered dinner invitations from male friends.
Meet Emily Williams

► Fictional CSE created to abstract sensitive information from a specific target. She graduated from MIT and had 10 years of experience despite she was 28 years old.

► Despite the fake profile, she was offered sensitive information from our target’s AM and CSEs. She had friends in large partner vendors and even offered dinner invitations from male friends.
The Impact of Social Media

► 10 minutes: 20 Facebook connections
   6 LinkedIn Connections

► 15 hours: 60 Facebook connections
   55 LinkedIn Connections

► 24 hours: 3 job offers

► Total Connections:
   170 Employees, 71 Cisco; 22 NetApp; 10 EMC; 35 McAfee; 300+ Facebook friends

► Endorsements:
   22 LinkedIn Endorsements, for Expertise and Experience; From Partners and Co-workers

► Offers: 4 job offers, Laptop and office equipment, network access.
Ahhhh that is so sweet! You are terrible at keeping secrets because I get really involved in your profile stuff. I... but I am SO excited to meet you! Please let me have fun :-(❤️❤️

---

Hi Emily,

Any chance you would be interested in a senior SE position? I think you would be a perfect fit. If you have a few minutes, can we schedule an interview at the office?

---

Emily

Men trust attractive women
**What did we do?**

**What?**

- Created fake FaceBook and LinkedIn profile to gain information using social media.

**How?**

- Social engineering techniques that allowed us to participate as a New Hire

**What was captured?**

- Salesforce Logins, Issued Laptops, Jobs offers, Endorsements, Meet up requests

**What was the real threat?**

- Published a Christmas card on social networks that gave us remote access to anyone that clicked on the link. This gave us significant access to devices and data.
Happy Holidays

Security in knowledge

RSACONFERENCE EUROPE 2013

#RSAC
Click Jacking

Attacked website is in a fully transparent IFRAME (it is not visible)

Malicious website

Train Your Brain!

97 + 3 = ?
203 - 3 = ?

Fake input controls with low Z index, positioned strictly "under" the hijacked web controls

User provides quiz answers, then hits the "Next" button.
All these clicks are hijacked by the invisible frame as its controls have higher (by default) Z order.

Image Copyright: ThreatExpert Ltd. 2008
Malware

Happy birthday to the best big bro ever!! Love you loads!! Aamir Lakhani
 [*] WE GOT A HIT! Printing the output:

 PARAM: userName=Ladi
 POSSIBLE PASSWORD FIELD FOUND: UserPassword=IloveToDance
 PARAM: target=%2f
 PARAM: Log+On.x=59
 PARAM: Log+On.y=10

 [*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
What does Emily Teach Us?

- Identities are a valuable commodity
- Humans are naturally trusting
- People use the same passwords for everything!
- Attractive women get special treatment in a male dominated industry
- Common security products will not protect you from Social Engineering
- Social Engineering threats can impact your business.
- There isn’t a silver bullet product that can protect you from a future
Emily Williams
When is helpful too helpful?

RE: Join my network on LinkedIn

Happy to be your valet when you arrive in ___________! Give me a little notice when your schedule is set. Do you need any help in getting the Service Desk to accelerate the laptop and email issues?

On 11/01/12 12:51 PM, Emily Williams wrote:

-----------------------------
Thanks Ecornell!

I am still get situated getting my laptop and email. I can't wait to get started! Are you in ___________? I think I will be coming up there soon to meet with a customer. You will definitely need to introduce me to everyone up there! :)

RSA Conference Europe 2013
Some people flagged suspicious activity.

Some people asked "Do I know you?"

Anyone ever had this happen? A person you don't know adds you that has a new profile with maybe 5 mutual friends – but no other friends. After they add you they start mass adding all of your friends. Other friends also email about the same thing – asking me how I know her. That's why I deleted her. Smells like a troll.

Like · Comment

4 people like this.

View all 11 comments

This is why I stopped posting to Friends of Friends and just do it to Friends now.
Yesterday at 12:35pm · Like · 1

Foff posting has definitely expanded my audience, but yeah... I have to deal with the BS sometimes.
Fortunately, I've been the Robin Hood of trolls since 89.
Yesterday at 12:37pm · Like · 1

Yes. Just today I was asked to be friends with 2 people I don't know. We only have one "mutual friend" between both of them. I just ignore them. I am considering thinning down the herd anyway, let alone adding new ones.
Yesterday at 12:44pm · Like · 1

That is why I don't allow many realtors to be my friend. I am a realtor, I have seen how some of them work.
23 hours ago via mobile · Like · 1
The Bad News
► We used Facebook and LinkedIn against you!
► What do you leave on social networks that could be used against you?

► We know your secrets.
► What did you wear on that date?
► It's not a secret anymore.

Emily Williams
I thought I knew you from Hungry Howie days

Emily Williams
Dang your right that was forever ago hahaha

Emily Williams
I hope life has treated you like gold!

Emily Williams
Yea it's been years. Ran into Derrick in NYC a while ago but outside that haven't seen people since I left b town

Emily Williams
Were still rockin it in b-town! I started my own business, and do Films now! I just finished my 3rd film acting, and am bout to direct my first, and am writing my first screenplay: ) I'm super excited!
Social Engineering Best Practices

- Segment the network
- Provide limited approved access
- Spread your security investments
- Next generation XYZ isn’t a silver bullet
- Attack your own network
- Use your data or its worthless
Big Data Security Analytics

► Hot, Warm, and Cold Data Threats
► Trending and Predictive Analysis
► Search “Kill Chain” on DrChaos.com
Social Engineering Countermeasures

- Question suspicious behavior
- Forward any possible threats to HR
- Be aware of what is public
- Never share work internals on social networks
- Protect your data with STRONG passwords.
- Don’t share devices used for work.

“On the Internet, nobody knows you’re a dog.”
Can’t Solve Every Problem
Thank you!

Aamir Lakhani
World Wide Technology
@aamirlakhani
www.DrChaos.com
www.wwt.com

Joseph Muniz
Cisco Systems

TheSecurityBlogger.com
www.cisco.com