Security 101

BY DAN WILKINS

I am an expert

NOT AT WHAT I WOULD HOPE


OISF

Recon

- Webster's Dictionary
  - A preliminary survey to gain information
- Sun Tzu
  - "Thus, what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge."
  - "If you know your enemies and know yourself, you will not be imperiled in a hundred battles... if you do not know your enemies nor yourself, you will be imperiled in every single battle."
- InfoSec
  - Find out everything you can before you go after the target

Do Not Share

We have made this so easy

Then

Now

So what information are we looking for?

Non-Technical

- Employee names
- Email addresses
- Titles and departments
- Physical location
- Phone numbers
- Any personal information (children, spouse, etc…)
- Tools they use (LinkedIn is great)
- Partner companies

Technical

- What sort of computers
- Usernames/Domain name
- Servers (DC, DNS, etc…)
- IP range
- Antivirus
- IPS/IDS
- SIEM
- VPN
- Policies (password, incident, etc)

Recon Demo

GO TO (*INSERT COMPANY NAME HERE) AND DO A LITTLE RECON

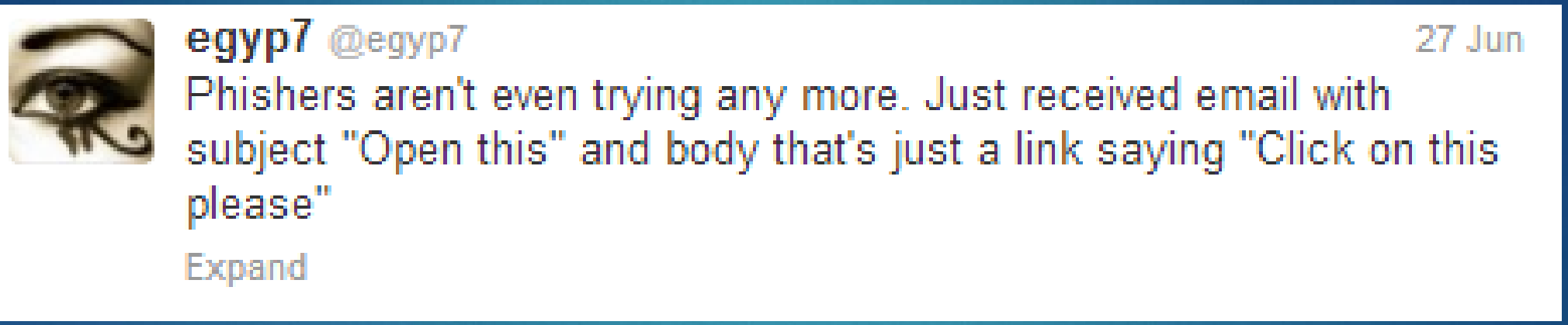
Social Engineering

- Definition
  - The art of manipulating people into performing actions or divulging confidential information.

- Kevin Mitnick—one of the most famous social engineers in the world—popularized the term "social engineering." He explained that it is much easier to trick someone into revealing a password for a system than to exert the effort of hacking into the system.

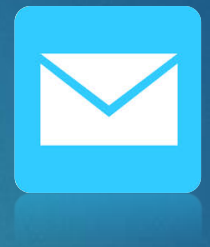
Social Engineering Fail

Social Engineering Fail



What does this include?

- Requesting information
  - Extensions
  - Voicemail
  - Business specific terms
- Convincing to action
  - Reset password
  - Run application
  - Go to website



- Phishing
  - Attachments
  - Links
- Information from replies
  - Especially autoreply
  - Signature information

Scenarios

- Think through some scenarios for your company
  - Outside in
  - 3rd party contractor
  - Insider attack

Demo of SE

DOES IT REALLY MATTER IF I CLICK ON THAT?

Password cracking

We still aren't getting it

Trustwave Survey top 10 2012

1. Password1
2. welcome
3. password
4. Welcome1
5. welcome1
6. Password2
7. 123456
8. Password01
9. Password3
10. P@ssw0rd

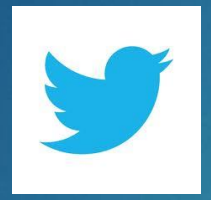
Yahoo accounts hack

1. 123456
2. password
3. welcome
4. ninja
5. abc123
6. 123456789
7. 12345678
8. sunshine
9. princess
10. qwerty

Weakest Link

Not Effective

Passwords get lost all the time



Tips for good passwords

- Use a different password for different applications
- Use a password manager
- Use strong passwords – Upper, lower, numbers and symbols
  - Instead of password - P@ssw0rd (don't use this…never use password)
  - @ for a, $ for s, 0 for o, 3 for e, etc…get creative
  - Use a phrase – TheBrownsWillNeverWin – ThBr0W1N3W1n
  - Make it longer than 8 characters

Password cracking demo

I DIDN'T SACRIFICE TO THE DEMO GOATS, SO LETS SEE HOW THIS GOES

Conclusions

- Be careful with the information you make available online
- Do not necessarily trust everyone that calls and requests information
- Don't use easy to guess/crack passwords
- Use 2 factor authentication if available
- Trust your judgment if a site seems fishy
- This is about your information as much as the companies, it isn't the guy in mom's basement anymore

- Have a Mohawk!

Next Steps

What they aren't

- More tools
  - Firewalls
  - IDS/IPS
  - Antivirus
- New Technology

What they are

- User awareness
- User training
- Defense in depth

What can we do?

- http://stopthinkconnect.org/
- http://www.staysafeonline.org/teach-online-safety/csave
- Password Vaults
  - LastPass - https://lastpass.com/
  - KeePass

Any Questions?

Dan Wilkins - http://about.me/cdjadex