BAKED NOT FIRED

UNAUTHORIZED PHISHING

BY

THE BOLLOCKS

- Undermine their pompous authority
- Reject their moral standards
- Make anarchy and disorder your trademarks
- Cause as much chaos and disruption as possible
- Don't let them take you ALIVE

- Sid Vicious

OR… MAYBE NOT

Sid Vicious seized at Chelsea Hotel

We believe his truth programming and the instructions to lie, gradually resulted in an incompatible conflict…

and faced with this dilemma, he developed, for want of a better description, neurotic symptoms.

THE INCOMPATIBLE CONFLICT

- Global company with a small security consulting group
- Good security policy but poor security awareness and practices
- HR loses unencrypted CD with employee SSNs
  - Policy explicitly states that this data should be encrypted
  - Past security awareness campaigns have communicated this policy
- Years of requesting a digital signature for corporate announcements
- No substantive response to underlying awareness and process problems

Normal communication is ineffective. Must try harder.

THE NEUROSIS

- Create a phishing e-mail announcing the Identity Theft Insurance vendor that was promised
- Create a phishing web site for collecting information
- Ask for Intranet logon information too

GOALS

- Raise security awareness
- Demonstrate that policy is no good without testing
- Create a branded security awareness process to give/sell to our customers
- Raise brand association with security within customer's minds

PRINCIPLES

- Only I take on any risk
  - No other employee should be an accessory
  - Phishing victims should not get in trouble for falling for it
- Make it as easy as possible for IT Security to respond
  - Document how it was set up
  - Give them the independent ability to shut it down
- Perhaps get fired, but not get prosecuted
  - Don't really collect anything
  - Don’t ask for anything that can’t be changed
  - Be as transparent as possible

EXECUTION DNS

- Register Domain with my name
- Create my-company branded domain name
- If possible use CNAME (or use A with stable IP) to Internal host for phishing server
  - No unencrypted sensitive information sent over the Internet
  - VPN connection allowed use of CNAME
  - Killing VPN connection removes phishing server

EXECUTION MAIL

- Find internal SMTP forwarder
- Use script to send mail, not telnet
- Test to myself, more than once
- Use traceable IP address to send SMTP
- Use plain text e-mail, nothing hidden
- Borrow as much language as possible from other official emails
- Don't forget Out of Office bounces

EXECUTION WEB SERVER

- Plain default Apache install
- Nothing else except the necessary files
- Used corporate laptop assigned to me for server
- No scripts unless already present in pages being borrowed.
- Make sure logs are clean, or turn off logging.

EXECUTION WEB PAGES

- Intranet logon page
  - POST to html, no cgi
  - Submit and cancel do the same POST
- Next page is purely educational
- Put notes in HTML source for investigators
  - Linked to “how this was done” documentation
- Test, test, test

LESSONS LEARNED

- Document more
- Unexpected actions create unpredictable responses.
- If they trust you, some won't believe it is you even when they see it is you
- Notify security directly, not just through web page documentation
- Make sure the site is secure (it got Web Inspected)

MORE LESSONS LEARNED

- Don't give in on the principles
  - I thought all connections would come from proxy, but it redirected to internal sites for many users.
  - Live IP PTR lookups could have revealed some who had visited
  - I refused to hand over the apache logs when asked by a manager who wanted to know which of his reports were caught.
- It may not be enough to protect victims from provable guilt
  - “They shouldn’t even click on cancel.”

NEVERMIND

THE QUESTIONS

BYE