Phishing Tips and Techniques

Tackle, Rigging, and How & When to Phish

Peter Gutmann

University of Auckland

Why can't users get security right?

Users are idiots

- Developers build security applications
- Users apply them incorrectly
- Users are idiots
- QED

Waitaminnit, they can't *all* be idiots…

- What's the pattern?

User Conditioning

"We can fix security problems with better user education"

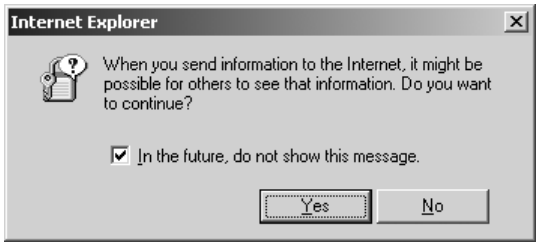
- We've been educating (conditioning) users for years…
- DNS errors, transient network outages, 404 errors, ASP problems, Javascript warnings, missing plugins, temporary server outages, incorrect or expired certificates, MySQL backend problems (any slashdotted site), …
- In all cases the solution is to click "OK"/"Cancel" or to try again later until it works
- Users have become conditioned to applying this solution to all computer/network problems

Network attacks exhibit identical symptoms to the above

- We're trying to detect attacks with a close to 100% false positive rate!

User Conditioning (ctd)

The following dialog pops up the first time the user searches ebay for dog food



- Note the "go away and don't bother me again" checkbox
  - Even the dialog's designers admit that it's just an annoyance
- No context for this: Could be a banking PIN or a dogfood query

User Conditioning Example

Large banking site

- Certificate had expired, leading to browser warnings for anyone who used the site
- Just one single user out of 300 turned away

  Hotmail does this all the time, you just wait awhile and it works again

  — User comment

User Conditioning Example (ctd)

Government site used to make multi-thousand-dollar property tax payments

- No-one was deterred by a large red cross and warning text indicating that the certificate was invalid

In a high false-positive environment like this, certificates are totally ineffective in providing security

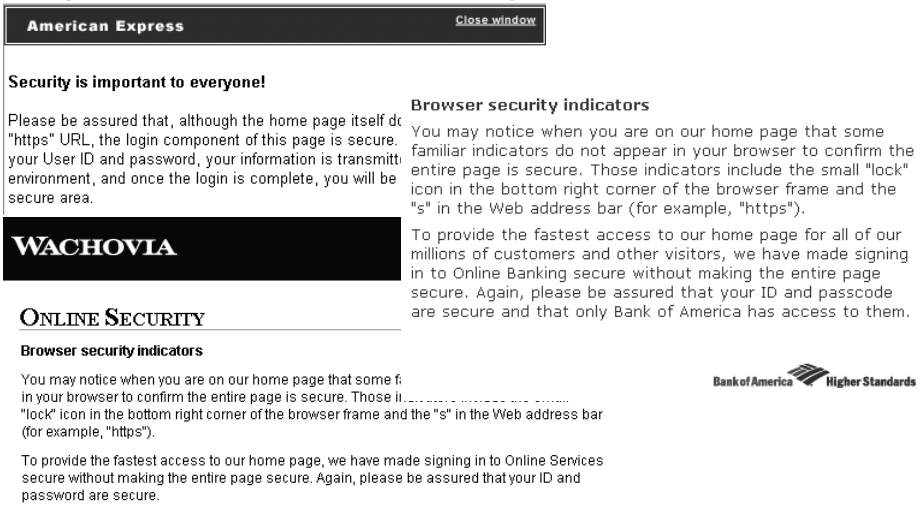
Phishing Tip

Invalid certificates don't bother users

- Create your own CA with any name that you want
- Use your CA to issue certificates for any web site you want
- More on this later

User Conditioning Example

Financial institutions are actively training their users to ignore certificate-based security indicators



American Express — Close window

Security is important to everyone!

Please be assured that, although the home page itself do "https" URL, the login component of this page is secure. your User ID and password, your information is transmitt environment, and once the login is complete, you will be secure area.

Browser security indicators

You may notice when you are on our home page that some familiar indicators do not appear in your browser to confirm the entire page is secure. Those indicators include the small "lock" icon in the bottom right corner of the browser frame and the "s" in the Web address bar (for example, "https").

To provide the fastest access to our home page for all of our millions of customers and other visitors, we have made signing in to Online Banking secure without making the entire page secure. Again, please be assured that your ID and passcode are secure and that only Bank of America has access to them.

Bank of America Higher Standards

WACHOVIA

ONLINE SECURITY

Browser security indicators

You may notice when you are on our home page that some f in your browser to confirm the entire page is secure. Those i "lock" icon in the bottom right corner of the browser frame and the "s" in the Web address bar (for example, "https").

To provide the fastest access to our home page, we have made signing in to Online Services secure without making the entire page secure. Again, please be assured that your ID and password are secure.

Phishing Tip

Target US financial institutions

- They have the worst online security practices of any banks
  - Users are heavily conditioned towards accepting these poor security practices
- Second-worst are UK banks
- Second-best are Australasian banks
- Best are European banks
  - PIN calculators, smart cards, TANs (one-time per-transaction PINs), …
  - Don't bother with these unless you really know what you're doing

Results of User Conditioning

SecuritySpace survey found that 58% of *all* SSL certificates were invalid (expired, self-signed, unknown CA, incorrect domain, etc)

- Most people only see the valid certs from big sites

2005 study found that invalid SSL certificates had no effect whatsoever on people visiting a web site

- Effect of certificates was indistinguishable from placebo

  Because most users dismiss certificate verification error messages, SSL provides little real protection against MITM attacks

  — Security study

Results of User Conditioning (ctd)

Honesty-box security

- Use a $495 Verisign certificate
  - People will come to your site
- Use a $9.95 budget CA certificate
  - People will come to your site
- Use a $0 self-signed certificate
  - People will come to your site
- Use an expired or invalid certificate
  - People will come to your site
- Use no certificate at all, just a disclaimer saying that you're secure
  - People will come to your site

Results of User Conditioning (ctd)

Even worse, users treated a site with no certificates as being less secure than one with an invalid certificate

- Users assumed that the mere presence of a certificate (even if it was invalid) made the site legitimate
  - Expired safety certificate in a lift/elevator doesn't mean that it's unsafe to use, merely that the operators forgot to get a new one
  - How many people even look at these sorts of certificates?
- This is *worse* than placebo!

  Users actually behaved less insecurely when interacting with the site that was not SSL-secured

  — Security study

Phishing Tip

Using a self-signed certificate gets you more respect than not using a certificate at all

- More on this later

In 2005 alone, 450 "secure phishing" attacks were recorded

- Self-signed certificates
  - Taking advantage of the "any certificate means the site is good" mindset
- XSS, frame injection, …
- Genuine certificates issued to soundalike domains
  - Fake site: `visa-secure.com`
  - Real Visa sites: `verifiedbyvisa.com`, `visabuxx.com`, …

How Users Make Decisions

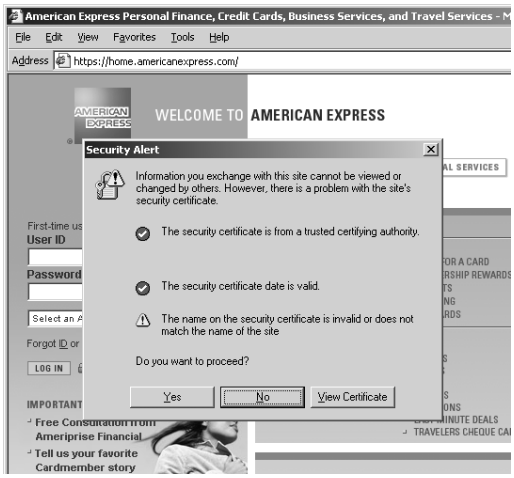
Recognition-primed decision making model

- Standard economic decision-making model assumed that someone making a decision
  - Weighs up a set of alternatives
  - Chooses the best one
- US DoD sponsored research into improving battlefield decision-making
- Found that users making a decision
  - Generate options one at a time, without ever comparing any two
  - Reject approaches that don't work
  - Take the first one that does
- Singular evaluation approach

How Users Make Decisions (ctd)

Singular evaluation is used when

- User is under pressure
  - Computer users wanting to do their job automatically fall into the "under pressure" category
- Conditions are dynamic, no time to perform detailed analysis



- Users have little basis for analysing/comparing choices
  - "certificate is for a different domain" → "eddies in the time/space continuum"

How Users Make Decisions (ctd)

Singular evaluation approach saves time and effort when dealing with pointless popup dialogs

- The web encourages this: If you make a mistake, click "Back" and try again (satisficing)

The ability to sort out relevant details from the noise is what makes it possible for humans to function

- Human senses filter light and sound to a manageable level
- Selective attention processes provide further filtering
  - Cocktail party phenomenon
- Forgetting discards non-useful information

How Users Make Decisions (ctd)

If humans didn't use singular evaluation, they'd never get anything done

- Attempts to computerise singular evaluation (a.k.a. "common sense") lead to programs that had to grind through millions of implications to find a solution
- AI researchers call this the frame problem
- In humans, it's a disorder called somatising catatonic conversion

Singular evaluation isn't a bug, it's what allows humans to function

Phishing Tip

This is not grumbling about idiot users, this is an immutable law of nature

- You cannot ignore, avoid, or "educate" users out of this
- This behaviour is not the exception, it's the environment

This isn't going to be patched in a hurry

- You cannot "solve" this human problem → target it as much as possible

Automatic Processes and Habituation

Controlled processes

- Slow
- Costly in mental effort
- Provide a great deal of flexibility

Automatic processes

- Quick
- Little mental effort
- Acting on autopilot

Novice vs.experienced driver

- Changing gears, checking the rear-view mirror is slow and manual or quick and automatic

Automatic Processes and Habituation (ctd)

Humans are creatures of habit

- Automatic processes are triggered by certain stimuli
- Very hard to stop
- User's aren't consciously aware of what they're doing

Once users become habituated into certain behaviour, it's almost impossible to break this conditioning

- Microsoft found that so many users reflexively closed the Windows automatic updates dialog that they converted it to nagware to prevent it from being bypassed
- Users just treated the security update dialog as another piece of popup noise to be clicked away

Automatic Processes and Habituation (ctd)

This was noticed a century ago by Gestalt psychologists

- Users resist attempts to change their behaviour even in the face of evidence that what they're doing is wrong
- Gestalt psychologists called this phenomenon "Einstellung"

Software vendors have tried to work around this

- Tip-of-the-day
- MS Office paperclip
  - OK, so that didn't work…

Consequences of Habituation

Humans are very bad at generating testable hypotheses

- People will try to confirm their hypotheses → confirmation bias
- People are more likely to accept an invalid but plausible conclusion than a valid but implausible one

Extreme case of rationalisation: Patients whose brain hemispheres had been physically separated

- Tell one half of the brain to do something
- Ask the other half why it's doing it
- Patients always had an explanation, even though the left half literally didn't know what the right half was doing

Consequences of Habituation (ctd)

Bank site located in eastern Europe

- Must be a problem with the server…
- The browser is displaying the URL wrong…
- It's some problem with the Internet…
- Yet another Windows bug…

As long as the site looks plausible, this will work

- Surely no-one would bother creating an entire fake site, would they?

Phishing Tip

People *want* to believe what they see

- Create a good enough copy of a site and it won't matter if it's hosted in Romania

The Simon Says Problem

Users are expected to change their behavior in the *absence* of a stimulus

- This is very, very hard to do

In web browsers, the absence of a (tiny) padlock is expected to change the user's behaviour

- The Hamming weight of the security indicator is close to zero
- A usability test of the IE6 SP2 security warning strip found that not one user noticed its presence
- In another test, no-one noticed a flashing message saying "There is a $50 bill taped to the bottom of your chair. Take it"
- In a test carried out by psychologists in 1999, only 43% of viewers noticed a person in a gorilla suit prancing around during a basketball game

The Simon Says Problem (ctd)

Humans have, as a part of their evolution, learned to focus on what's important

- Flashing lights
- Snakes, tigers, wolves
- Used-car salesmen

A small padlock or blue bar isn't important, and isn't noticed

Phishing Tip

Don’t worry about the MSIE 6 SP2 security ribbon and similar “phishing” indicators

- Most users simply won’t notice it
- The few that notice it won’t know what it signifies

US banks are working hard to train users to ignore these indicators anyway

Why can’t users get security right (revisited)

~~Users are idiots~~

Security people are wierdos

- Go directly against millennia of evolutionary conditioning
- No normal person would ever handle a user interface the way that security people do

Security people design these interfaces assuming that they’ll be used they way they would use them

- Security theory, meet the real world

Brand Power

CAs have attempted to introduce “high-assurance” certificates

- High assurance that you’ll be charged more for them

Many users don’t even know what a CA is

- No users know all of the 40-50 CAs hardcoded into their browsers

The most insignificant mainstream brand has more market presence than the most significant CA brand

- More people recognise Visa as a trusted CA than Verisign
- Verisign is the world’s largest CA
- Visa isn’t a CA at all

Phishing Tip

Create your own CA belonging to a major brand

- Use that CA to issue site certificates for the brand
- Do you want to trust `https://www.visa.com`, certified by the Visa CA?
  - Of course I do, it’s Visa!

Summary of Phishing Tips

Create your own CA for a well-known brand

- Use brand power to your advantage

Certify your phishing site using this CA

- Users are more likely to fall for your phish if you have any kind of certificate

Make it as close to the real thing as possible

- Take advantage of confirmation bias/inability to generate testable hypotheses

Summary of Phishing Tips (ctd)

Use US banking disclaimers about lack of security indicators

- US banks have done a lot of user conditioning for you

Don’t sweat the small stuff (padlocks, security ribbons, other indicators)

- No-one notices these anyway. Make the Simon Says problem work for you

Remember, you only need a 1% success rate

- They need a 100% success rate