Phishing Tips and Techniques

Tackle, Rigging, and How & When to Phish

Peter Gutmann

University of Auckland

Background

Phishing is currently the most widespread financial threat on the Internet

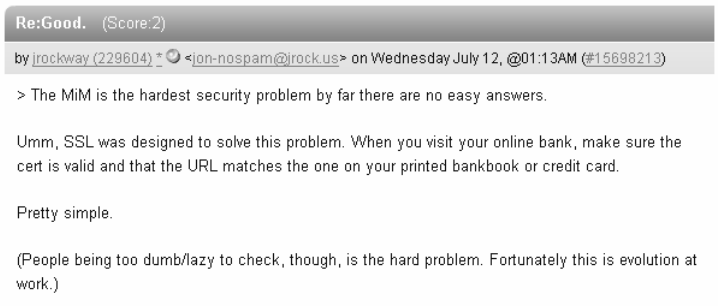
- Phishing sites increased at 28% / month in 2004-2005
- It's a $xB / year industry
- We know that it works
- We don't know why it works
  - "Users are idiots" isn't a reason

Why does it work?

- What are the threats?
- Where are the weak points in our defences?

Why can't users get security right?

Users are idiots



Re:Good. (Score:2)

by jrockway (229604) * <jon-nospam@jrock.us> on Wednesday July 12, @01:13AM (#15698213)

> The MiM is the hardest security problem by far there are no easy answers.

Umm, SSL was designed to solve this problem. When you visit your online bank, make sure the cert is valid and that the URL matches the one on your printed bankbook or credit card.

Pretty simple.

(People being too dumb/lazy to check, though, is the hard problem. Fortunately this is evolution at work.)

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

Why can't users get security right? (ctd)

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

> Look at all these idiots driving the wrong way down the motorway, I'm the only one going in the right direction

If everyone's getting it wrong, there's a problem with the design / implementation

Why can't users get security right? (ctd)

Developers have created a pile of security widgets for browsers and similar applications

- Padlock icon
- 'https://' indicator
- Coloured URL bar
- Certificate warnings
- (Optional) security toolbars

None of this was ever really tested on users

> If users don't understand it, it doesn't exist
> — Security HCI prime directive

Why can't users get security right? (ctd)

When it was finally tested (ten years after it was introduced), the results were disturbing

- 65% ignored the padlock
- 59% paid no attention to the 'https://' indicator
- 77% didn't notice the address bar colouring
  - Of those who noticed it only two understood its significance
- When presented with a certificate warning dialog, 68% immediately clicked 'OK' without reading the dialog
  - Just one user was able to explain what they'd just done

Why can't users get security right? (ctd)

Another study found that not a single user checked the certificate when checking site validity

Yet another study found that only 18% of users could identify an unprotected (SSL vs. no SSL) site

And yet another study found that […]

OK, we get the picture, it doesn't work!

User Conditioning

"We can fix security problems with better user education"

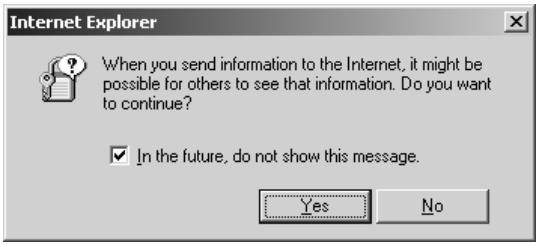
- We've been educating (conditioning) users for years…
- DNS errors, transient network outages, 404 errors, ASP problems, Javascript warnings, missing plugins, temporary server outages, incorrect or expired certificates, MySQL backend problems (any slashdotted site), …
- In all cases the solution is 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)

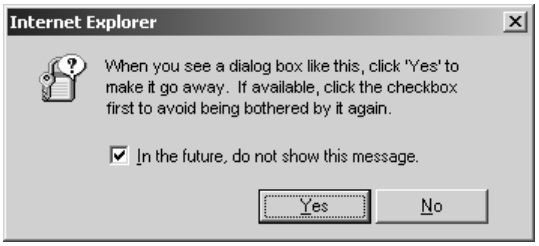
The following dialog pops up the first time the user searches ebay for dog food



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

User Conditioning (ctd)

Effect of this dialog on users



- The actual text is irrelevant, *this* is what the user absorbs
- A Win95 beta dialog told users "in order to demonstrate our superior intellect, we will now ask you a question you cannot answer"
  - Again, the dialog's designers knew exactly what they were asking of users

User Conditioning (ctd)

An entire generation's computing experience is built around clicking 'OK' to error messages that they don't understand

- In a standard HCI context, this would be just moaning about bad UI design
- In a security HCI context, this is phishing's primary attack vector
- You can take this principle to the bank — and the phishers are

User Conditioning Example

Large banking site

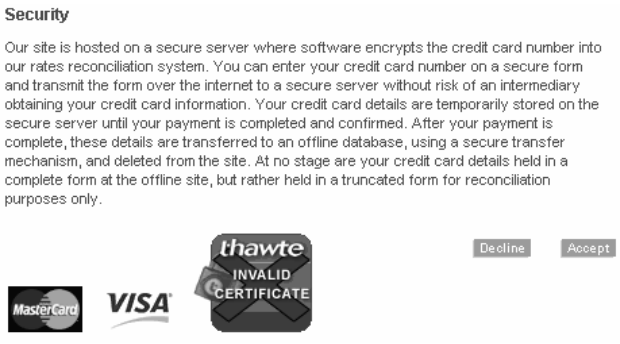
- Certificate had expired, leading to browser warnings for anyone who used the site
- Just one single user out of 300 turned away

  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
- All the security mechanisms were working exactly as designed

User Conditioning Example

SSL security depends entirely on user handling of certificates

- Leaves it up to the user to make the final decision

Security =

- AES-256 +
- RSA-2048 +
- SHA-1 +
- User judgement call

You can see why the attackers are going for phishing

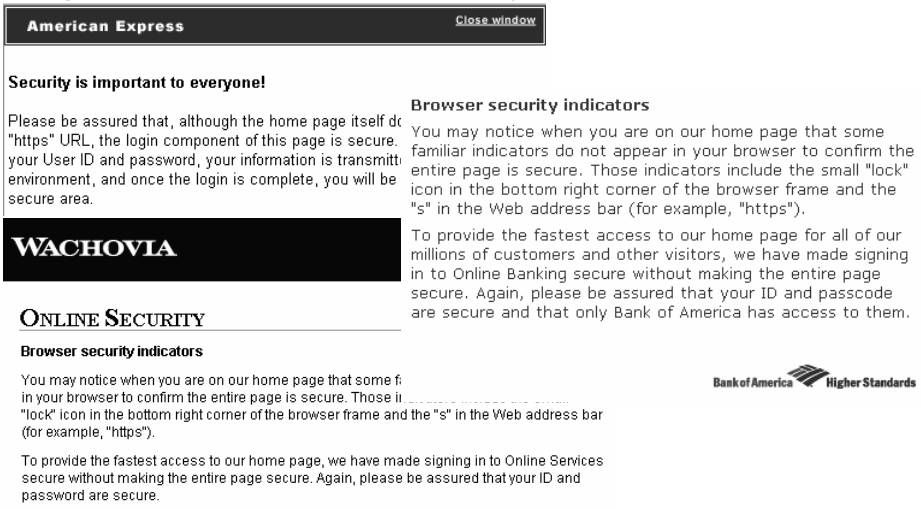
Phishing Tip

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

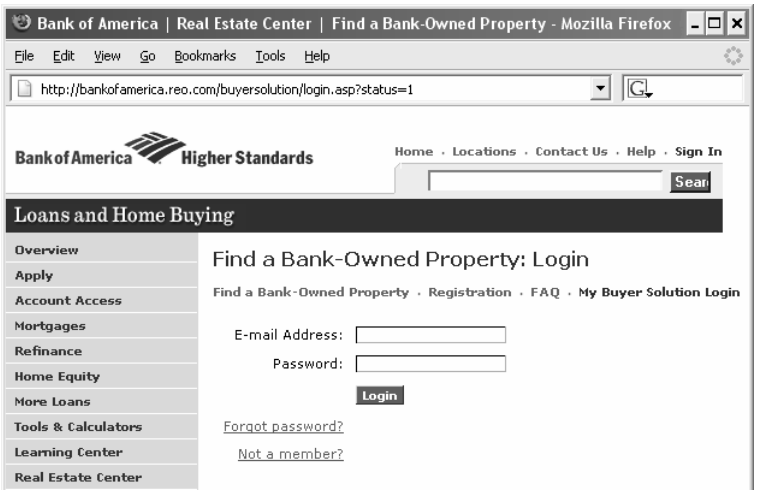
You may notice when you are on our home page that some f in your browser to confirm the entire page is secure. Those i "lock" icon in the bottom right corner of the browser frame and the "s" in the Web address bar (for example, "https").

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.

User Conditioning Example

They practice what they preach…

User Conditioning Example (ctd)



This is a genuine Bank of America site

- It just happens to be at `reo.com`

User Conditioning Example (ctd)

Bank emails are indistinguishable from phishing emails

> Customers should understand that Citibank will never send e-mails to customers to verify personal and/or account information […] It is important you disregard and report e-mails which […] request any customer information — including your ATM PIN or account details
>
> — Citibank Australia
>
> Go to *URL* and […] to identify and authenticate yourself, enter (a) your card number (b) your ATM PIN (c) your account number
>
> — Citibank Australia email, November 2006

User Conditioning Example (ctd)

> It had all the classic signs. It was an e-mail asking the customer to go to a Web site and enter their ATM or credit card number, their ATM PIN and their account number. It then asked them to enter some answers to security questions such as their mother's maiden name and create a username and password
>
> — Bronwyne Edwards, SMS Management & Technology

User Conditioning Example (ctd)

The bank couldn't see a problem

> Are you guys on crack?
>
> — Paraphrased journalist inquiry to Citibank
>
> These are all online banking customers and are used to receiving e-mails from us. I don't believe we have contradicted [our security policy]
>
> — Citibank Australia spokesperson

User Conditioning Example (ctd)

A profusion of domain names serve to confuse users

- `citibank.com` = Citibank
- `citibank-verify.4t.com` = Not Citibank
  - No problem to obtain a legitimate certificate for 4t.com

- `accountonline.com` = Citibank again
  - Citibank uses six more domain names

User Conditioning Example (ctd)

The Citibank namespace alone includes

citibank-america.com, citibank-credicard.com, citibank-credit-card.com, citibank-credit-cards.com, citibank-account-updating.com, citibank-creditcard.com, citibank-loans.com, citibank-login.com, citibank-online-security.com, citibank-secure.com, citibank-site.com, citibank-sucks.com, citibank-update.com, citibank-updateinfo.com, citibank-updating.com, citibankaccount.com, citibankaccountonline.com, citibankaccounts.com, citibankaccountsonline.com, and citibankbank.com

Most of these are highly questionable

- citibank-account-updating.com is owned by Ms. Evelyn Musa (Nigeria), ezayoweezay_halobye@yahoo.com.

User Conditioning Example (ctd)

Even legitimate domains are a mess

Hanscom Federal Credit Union (serving the massive Hanscom air force base, a tempting target) uses

www.hfcu.org, locator.hfcu.org, ask.hfcu.org, calculators.hfcu.org, www.loans24.net, hfcu.mortgagewebcenter.com, secure.andera.com, secure.autofinancialgroup.com, hffo.cuna.org, www.cudlautosmart.com, www.carsmart.com, reorder.libertysite.com, www.ncua.gov, www.lpl.com, anytime.cuna.org, usa.visa.com, and www.mycardsecure.com

Phishing Tip

Target US financial institutions

- They have the worst online security practices of any banks anywhere
  - Users are heavily conditioned towards accepting these poor security practices
- Second-worst are UK banks
  - Heise Security/UK found that six of the nine largest UK banks were trivially vulnerable to frame spoofing/cross-site scripting
    - Phishing sites were indistinguishable from the real thing
  - Two banks subsequently fixed their pages
    - Only one of the fixes actually worked

Phishing Tip (ctd)

Avoid Australasian/European financial institutions

- 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, so this problem isn't very visible

Browser vendors can't afford to fix this any more

- The majority of web sites would break
- "Microsoft is using its monopoly position to force people to go with commercial CAs"
- "Firefox/Opera/Safari can't access site X, MSIE can. Firefox/Opera/Safari is broken"

Results of User Conditioning (ctd)

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)

SSL certificates provide 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)

Study found that 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?
- How many people check that they match the building/elevator they're in, and are currently valid?

Results of User Conditioning (ctd)

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

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

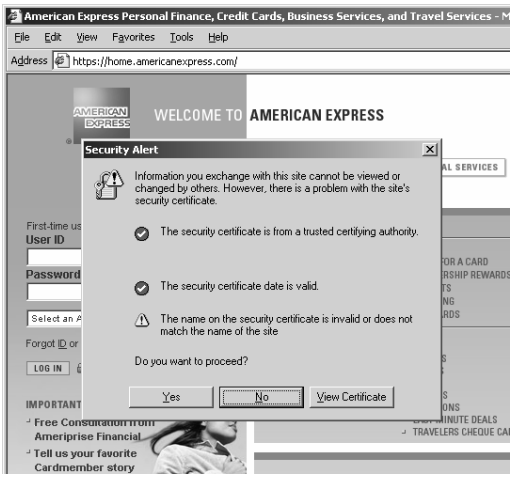
- Found that users making a decision
  - Generate options one at a time, without ever comparing any two
  - Reject approaches that don't work
  - Take the first one that does

This is termed the 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 is used constantly when dealing with computers

- Saves time and effort when dealing with pointless popup dialogs

The web browsing model encourages this poke-and-hope approach

- If you make a mistake click “Back” and try again
- Satisficing, an approach that both satisfies and suffices

Web users are deeply immersed in a singular-evaluation environment

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

How Users Make Decisions (ctd)

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

- Researchers performed an experiment where users were told to carefully evaluate a site
- Found that users spend "absurd amounts of time" trying to verify its legitimacy
  - Experiment had to be aborted
- False positive rate rose to 63%
  - If you look hard enough, you'll always find something suspicious

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 can't "solve" this human problem → target it as much as possible
- Sales people already know about forcing people into singular evaluation mode: "call in the next 10 minutes", "offer ends Monday", "try our exclusive …", …

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, looking left and right at intersections is slow and manual or quick and automatic

Automatic Processes and Habituation (ctd)

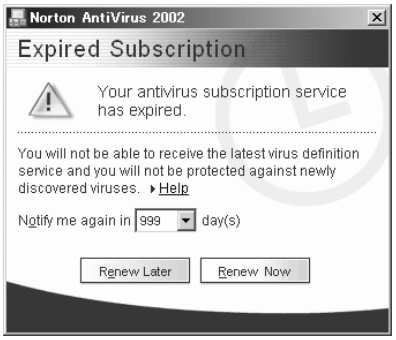
Humans are creatures of habit

- Automatic processes are triggered by certain stimuli
- Very hard to stop
- User's aren't consciously aware of what they're doing
  - "Did I lock the front door?"
  - "Did I leave the iron on?"

Automatic Processes and Habituation (ctd)

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

Users are required to endlessly authenticate themselves

- Browsers make no distinction between security levels
  - Firefox master password could be unlocking your bank account or your knitting patterns

Consequences of Habituation (ctd)

Even the legitimate application's requests for passwords are incomprehensible to any normal human

- "Eddies in the time/space continuum! Gimme your password"

Consequences of Habituation (ctd)

Users are habituated into entering their password for everything they do

- 2006 study found that 96% of users re-use passwords across sites
- Most users don't understand the consequences of password cross-pollination, and don't protect low-value accounts much

Roll on biometrics!

- Far more vulnerable than password authentication

Phishing Tip

Try an indirect phish for a low-value site

- Who cares about my password for knitting patterns?
- (Not too necessary yet since direct phishing is still so easy)

Try phished credentials at high-value sites

- Hotmail ID at Paypal, Bank of America, Wachovia, …

Reject the first few passwords that the user enters

- Automatic process conditioning: Did I enter the password for the right site?
- Users are so accustomed to entering passwords that they'll switch to other ones thinking that they used the wrong one

Phishing Tip

Try for the backup password (password hint)

- Many accounts have two passwords, the standard one and a (very weak) backup
- These are uniformly terrible
  - "What's your dog's maiden name?"

Real or Fake?

Humans are very bad at generating testable hypotheses

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

How do you check whether a site is for real?

- Enter your username and password
- If it lets you in, it's real

(If security people had bothered to implement password authentication properly, this would be a valid test)

- TLS-PSK provides mutual authentication of client and server
- Have the technology fit the user, not the other way round

Real or Fake? (ctd)

Extreme case of rationalisation: Patients whose brain hemispheres had been physically separated (corpus callosotomy)

- 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

Real or Fake? (ctd)

You can experience this yourself through visual "blind spot" tests

- Brain invents stuff to fill the blind spot where the optic nerve enters the retina

Other examples of the mind making things up

- Confabulation across saccades
- Filling in words in sentences that have been obliterated by a noise like a cough
- (Many others, this is a fun topic for experimental psychologists)

Real or Fake? (ctd)

Bank site located in an unexpected place

- `www.ssl-yahoo.com` is a subdirectory of Yahoo, like `mail.yahoo.com`
- `sign.travelocity.com.zaga-zaga.us` must be an outsourcing site for `travelocity.com`
- Sometimes the company has to register a different name [`www.mytargets.com`] from its brand. What if `target.com` has already been taken by another company?
- Sometimes I go to a website and it redirects me to another address
- I have been to other sites that use IP addresses

All of these are real responses from users in security studies

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

Make it easy to "confirm" the site's authenticity

- Inability to create a testable hypothesis means that counterindications are never explored

The Watermark Fallacy

Financial institutions have invested a great deal in anti-counterfeiting technology

- Intaglio printing
- Watermarks
- See-through register
- Rely on the difficulty of replicating physical artifacts

People assume that complexity implies authenticity

- "No-one would be able to replicate this Flash animation"
- Assume that the digital world follows physical copying rules

The Watermark Fallacy (ctd)

Sometimes not even complexity is required

- Holdover from the pre-computer age
- "Security by letterhead" was relatively robust when printing was hard
- Internet storefronts don't correspond to physical storefronts

Exploit the watermark fallacy

- Copy and prominently feature Flash, animated graphics, …

Be careful with too-literal copies

- Need to adjust ephemeral information like dates on copied pages

Phishing Tip

As long as the site looks plausible, this will work

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

Phishing Tip (ctd)

Federal Financial Institutions Examination Council (FFIEC) required that banks introduce two-factor auth

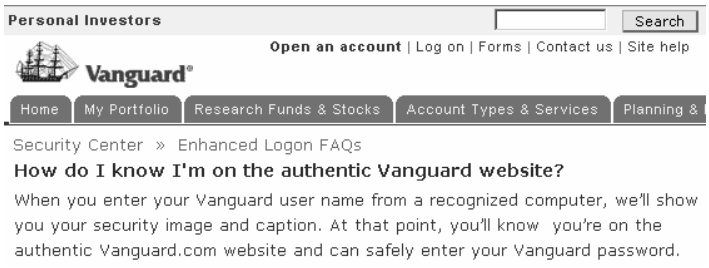
- Banks redefined "two-factor" to "twice as much one-factor"

Example: Bank of America uses SiteKey two-stage signon

- Users are directed to an intermediate page that contains a personalised graphic
- Serves no useful purpose since the initial page still isn't protected

Phishing Tip (ctd)

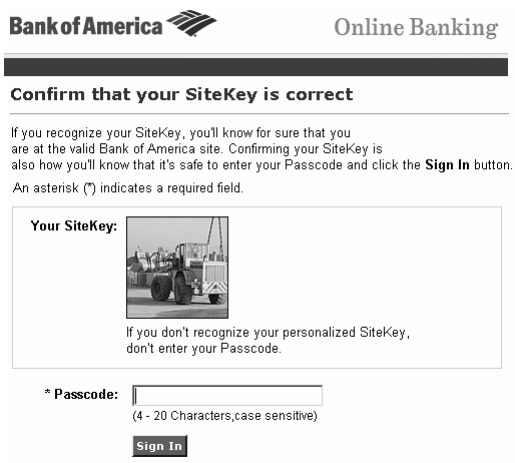
But wait… there's more…



The SiteKey message is training users to ignore SSL security indicators in favour of (ineffective) SiteKey ones!

Phishing Tip (ctd)

This pretend two-factor authentication is actually worse than the original purely one-factor form



Phishing Tip (ctd)

To bypass SiteKey-type "security"

- Use MITM to fetch the graphic from the real site
- Display a broken-image icon on the intermediate page
- Display "Your security settings have prevented this image from being displayed"

Independent evaluation found that even the simplest of these (the last one) convinced 92% of users that the site was genuine

- Gimmick security mechanisms of this type are rarely tested by vendors

Phishing Tip (ctd)

These gimmick mechanisms have a net negative effect on security

- Mechanism provides no value itself, but degrades other security mechanisms

In any case malware isn't even bothered by this

- Trojans include "grabbers" that hook into the Javascript engine and bypass AJAX-based additional "authentication"

The Watermark Fallacy Reloaded

Other factors that convince users that a site is genuine…

Correct spelling and clean layout

- (Poor English still works against victims whose 2nd/3rd language is English)

Personalisation

- "Love, John Smith" rather than "Sincerely, Mgr., Accounts Receivable"

Simple unprotected URLs trump complex SSL URLs

- `http://www.attuniversalcard.com` rated significantly higher in user testing than `https://www.accountonline.com/-View?docId=Index&siteId=AC&langId=EN`

The Watermark Fallacy Reloaded (ctd)

Pseudo-personalisation of communications

- Use geolocation to get the (US) Zip code
  - Some malware already does this
- Display the credit card prefix
  - 4828-****-****-****
  - Prefixes are shared across large numbers of users
  - Targeting specific banks allows you to use the banks' card prefix

Legal disclaimers and copyright notices

- "Phishers don't need legal disclaimers, so they won't include them in their messages"

The Watermark Fallacy Reloaded (ctd)

Out-of-band verification channels

- Display a phone number to call for a safety check

No-one calls it, they all assume that someone else will check

- In any case, phishers have set up their own IVR systems that mimic the banks' ones

The Watermark Fallacy Reloaded (ctd)

This phenomenon is so common that it has a name: the bystander effect

- The more bystanders, the less chance of any one individual taking any action
  - 85% with one bystander, 62% with two, 32% with five
- On the Internet, the bystander count is the *entire world*

The "someone else's problem" fallacy, also found in OSS security software

- "I won't trust it unless there's source code available, but I'll assume that someone else has checked it"
- Security holes have persisted in OSS security apps for years until they were found, often by chance

Privacy Seals: Security Chicken Soup

Theory: Sites apply for Better Business Bureau-style certification

- Guarantees that they meet certain minimal requirements
- Certification is withdrawn if they fail an audit

Practice: Anyone can get a seal

- Too many organisations selling them
- For some the only thing they demonstrate is that money changed hands (*cough*TRUSTe*cough*)
  - TRUSTe basic seal merely confirms that the site has a security policy of some form
  - "Our policy is to hand over all your private data to the Russian mafia" would qualify

Privacy Seals: Security Chicken Soup (ctd)

Common among scammers and fly-by-night traders

- So widely used that it has its own name, "seal abuse"
  I can get you any result you like / Whats it worth to you?

Verified by Visa, Diners, MasterCard, Verisign Secure Site, Better Business Bureau (BBB), various medical certifications (for dodgy pharmaceuticals), etc

Phishing sites can't have their seals revoked

- Variation of the watermark fallacy

Privacy Seals: Security Chicken Soup (ctd)

Users seem to like seeing them on web pages

- One study found that 42% of users said they'd trust a site more if they saw a trust mark
  - 49% if it was one that they recognised

Chicken soup, can't hurt to add them to your phishing site

Phishing Tip

The Simon Says Problem

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

- This is very, very hard to do

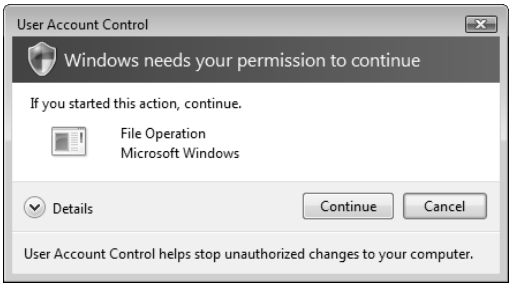
In web browsers, the absence of a (tiny) padlock is expected to change the user's behaviour

- The Hamming weight of the security indicator is close to zero

The Simon Says Problem (ctd)

A usability test of the IE6 SP2 security warning strip found that not one user noticed its presence

User reaction to Vista UAC colours: "There are different colours?"



- Now try and figure out what the colours signify

The Simon Says Problem (ctd)

In another test during usability evaluation of spreadsheet software, 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)

The ability to focus on a single target and 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

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 them
- The few that notice them won't know what they signify
- Security toolbars aren't installed by default
- 39% of users of various anti-phishing toolbars were fooled by phishing sites even after being told that they were part of a phishing study

US financial institutions are working hard to train users to ignore these indicators anyway

Brand Power

CAs have attempted to introduce "high-assurance" certificates

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

Most users don't even know what a CA is

- Term is only defined for locale = xx-geek
- No users know all of the 100-150 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!

Phishing Blacklists

Added to both MSIE 7 and Firefox 2

Implementation of "enumerating badness"

- No.2 on Marcus Ranum's "Six Dumbest Ideas in Computer Security"
- Actually a special case of default-allow, the No.1 dumbest idea

To sidestep this, just avoid the blacklist

- 0-day phish
  - Anti-Phishing Working Group reports that the average phishing site lifetime is 5 days
  - Spammers are already using sites with 6-hour lifetimes
- Reverse proxy via a botnet
  - Try blacklisting 10,000 constantly-changing IP addresses

Phishing Blacklists (ctd)

"But it works with virus scanners!"

- Virus scanners only have to find a virus in 100K files on a hard drive
- Even then, the most popular scanners have an 80% miss rate (AusCERT)
- Virus writers test their malware against the market leaders to make sure that it's not detected

  I had a class full of students this semester […] the second assignment was to write a virus that would pass the anti-virus software, and all of them did by the following week

  — Matt Blaze, 2004 Security Protocols workshop

Phishing Blacklists (ctd)

Phishing blockers have to detect a site among 1+ billion constantly-changing Internet-connected machines

- You'd have to monitor every machine all of the time and be able to blacklist them in close to real-time

Phishing Tip

Nothing to worry about

- Just make sure that your site isn't around long enough to be blacklisted
- Many sites are already doing this anyway

Like WW2 German superguns

- Working on it diverts resources away from solving the real problem

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 the way that they would use them

- At least one user study on PKI un-usability was greeted with disbelief by security people
- It couldn't possibly be this hard to use!

Why can't users get security right (revisited)

What the developers wrote

Why can't users get security right (revisited)

What the users read

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

Use an indirect phish (low-value credentials at high-value site)

- Users don't understand password cross-pollination

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)

Copy and feature Flash, animated graphics, …

- Leverage the watermark fallacy

Preferentially target US financial institutions

- Worst security of financial institutions anywhere

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

Summary of Phishing Tips (ctd)

Use short-lived sites/reverse proxies via botnets to avoid blacklists

If users don't understand it, it doesn't exist

- Look for studies showing poor usability of security features

Remember, you only need a 1% success rate for a successful phish

- The defenders need a 100% success rate

More Information

Slides available from my home page,
`http://www.cs.auckland.ac.nz/~pgut001`

Lengthy discussion of problems and countermeasures available from the same site,
`http://www.cs.auckland.ac.nz/-~pgut001/pubs/usability.pdf`