Phishing and Pharming

Sid Stamm
Indiana University

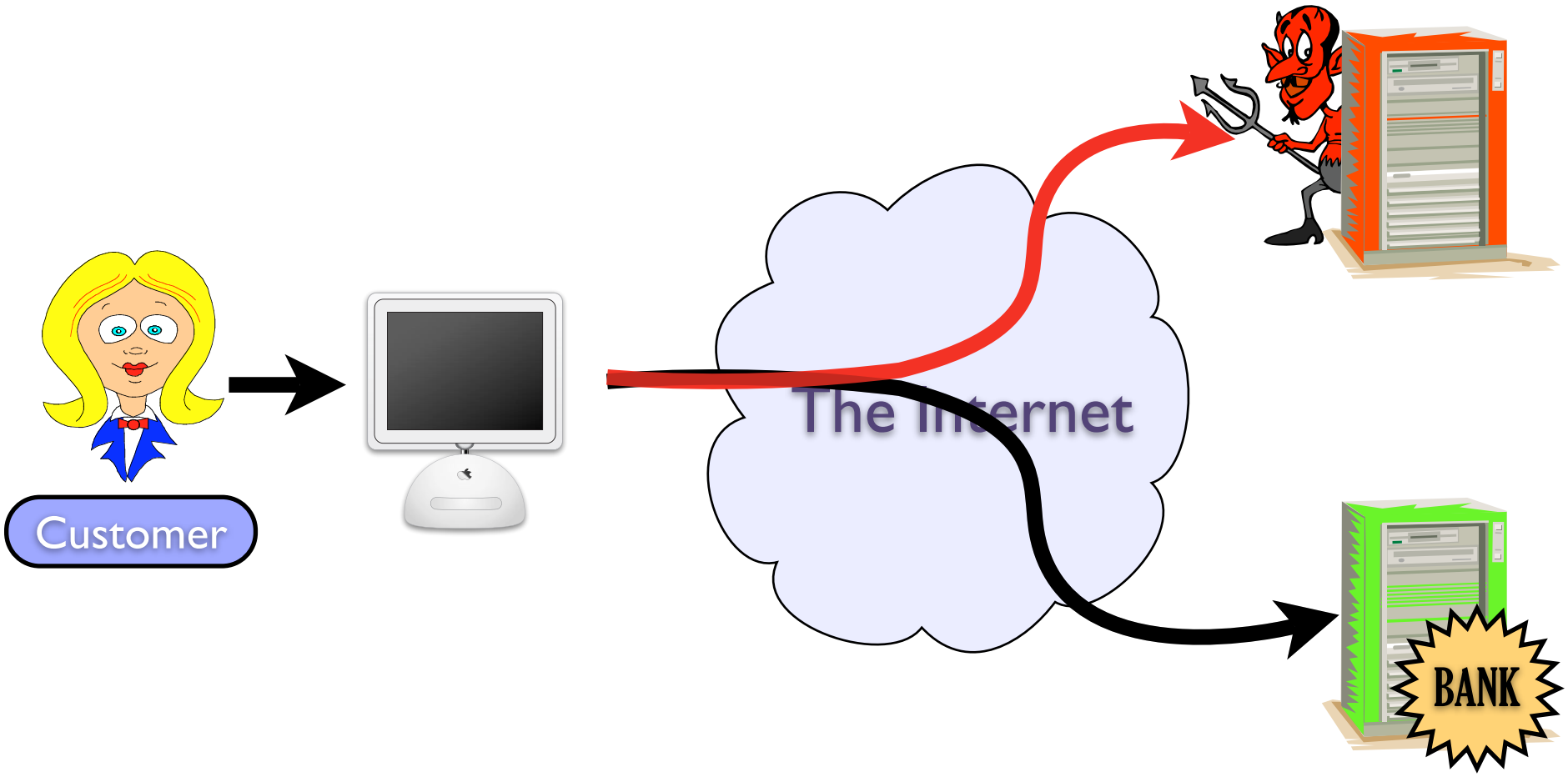
Warm up with a mention of how it is important to bring real life to research and vice versa... Am enjoying seeing a different perspective, hope I can offer one too.

Most of the time people realize something is phishing because the bank name is wrong -- this leads to context aware phishing (browser-recon, chameleon email based on browsing history -- webmail)

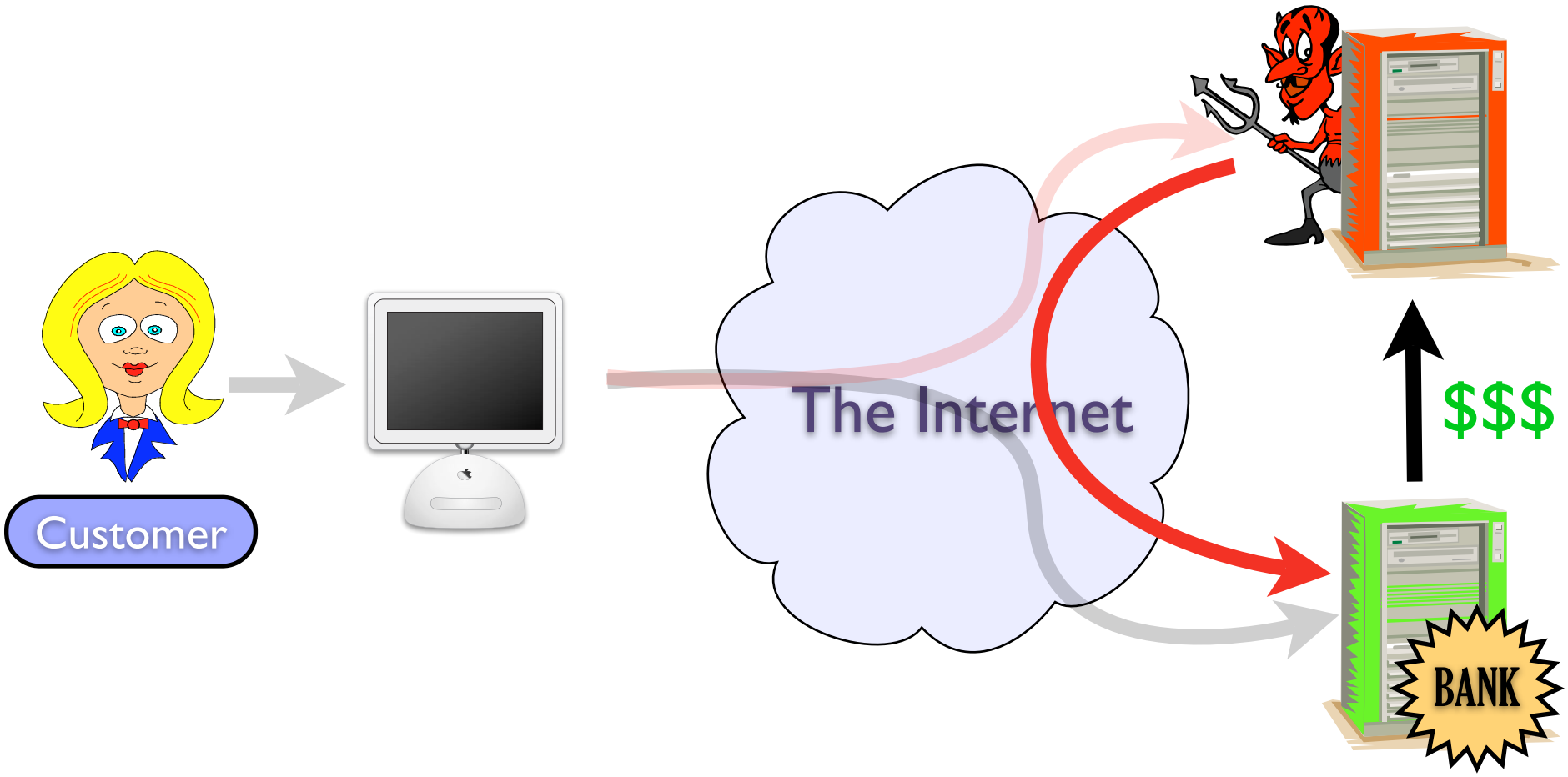
OUTLINE:

1. Threats/Attacks and specific examples
2. The human factor -- where your brother joe comes into play
3. Countermeasures for attacks and how they fail to solve the problems
4. Upcoming advances in phishing and pharming

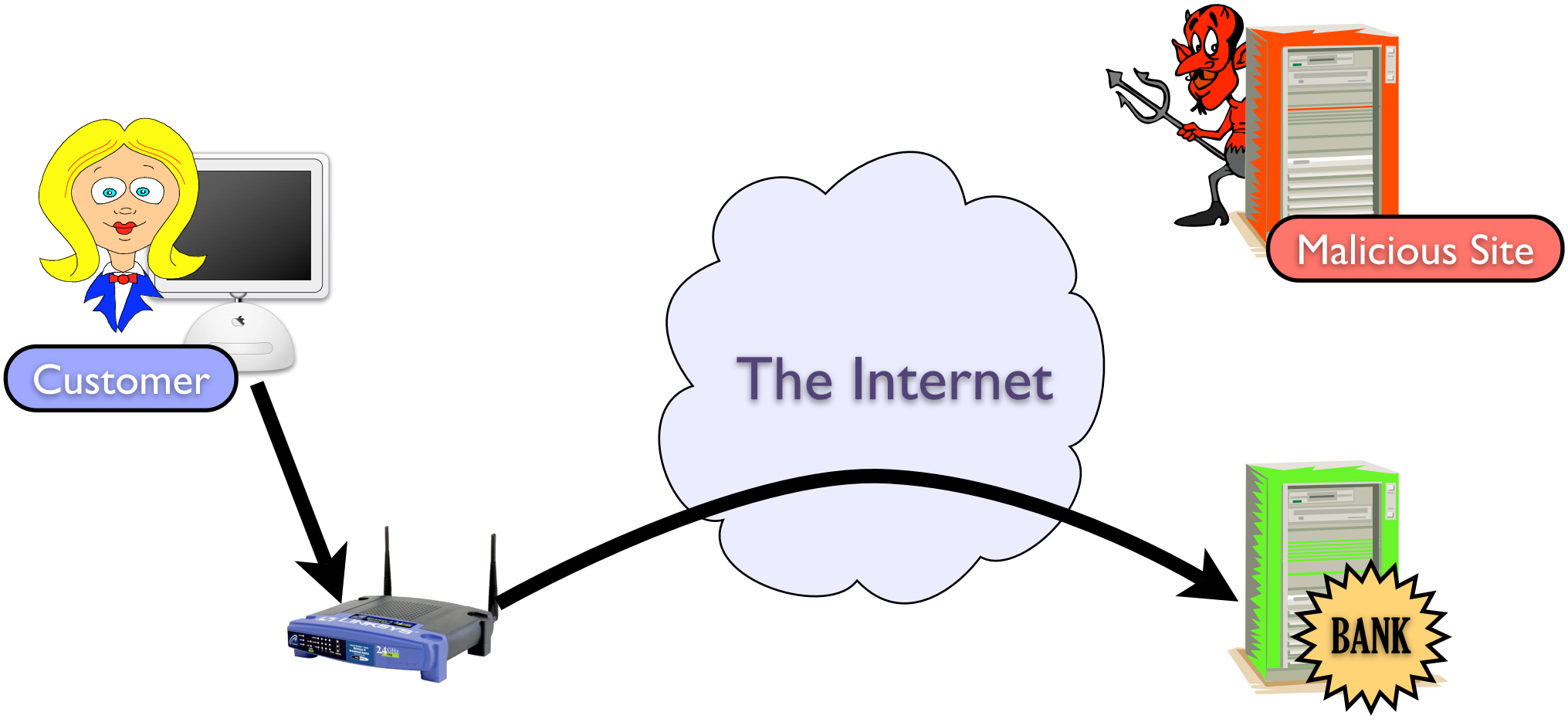
Attack!



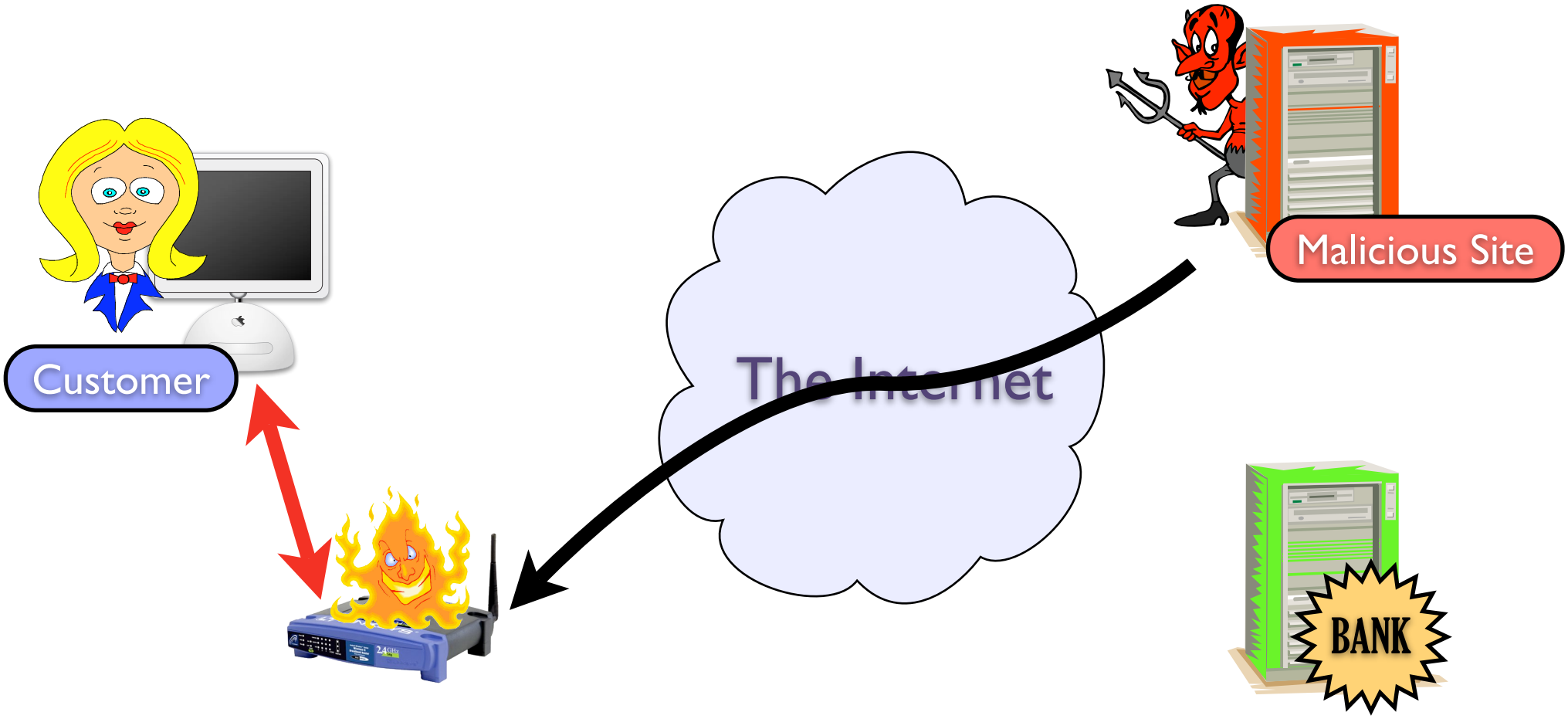
Attack!



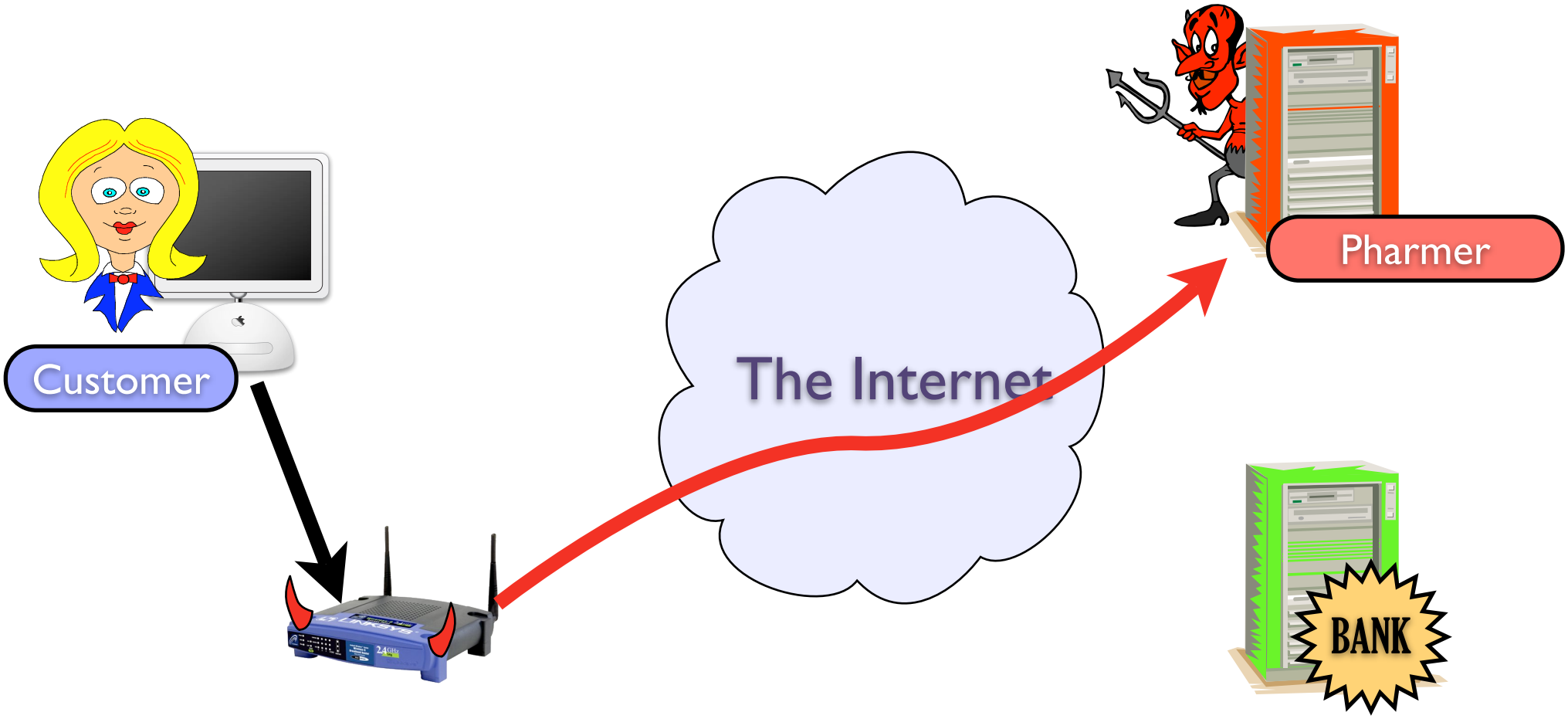
Drive-By Pharming



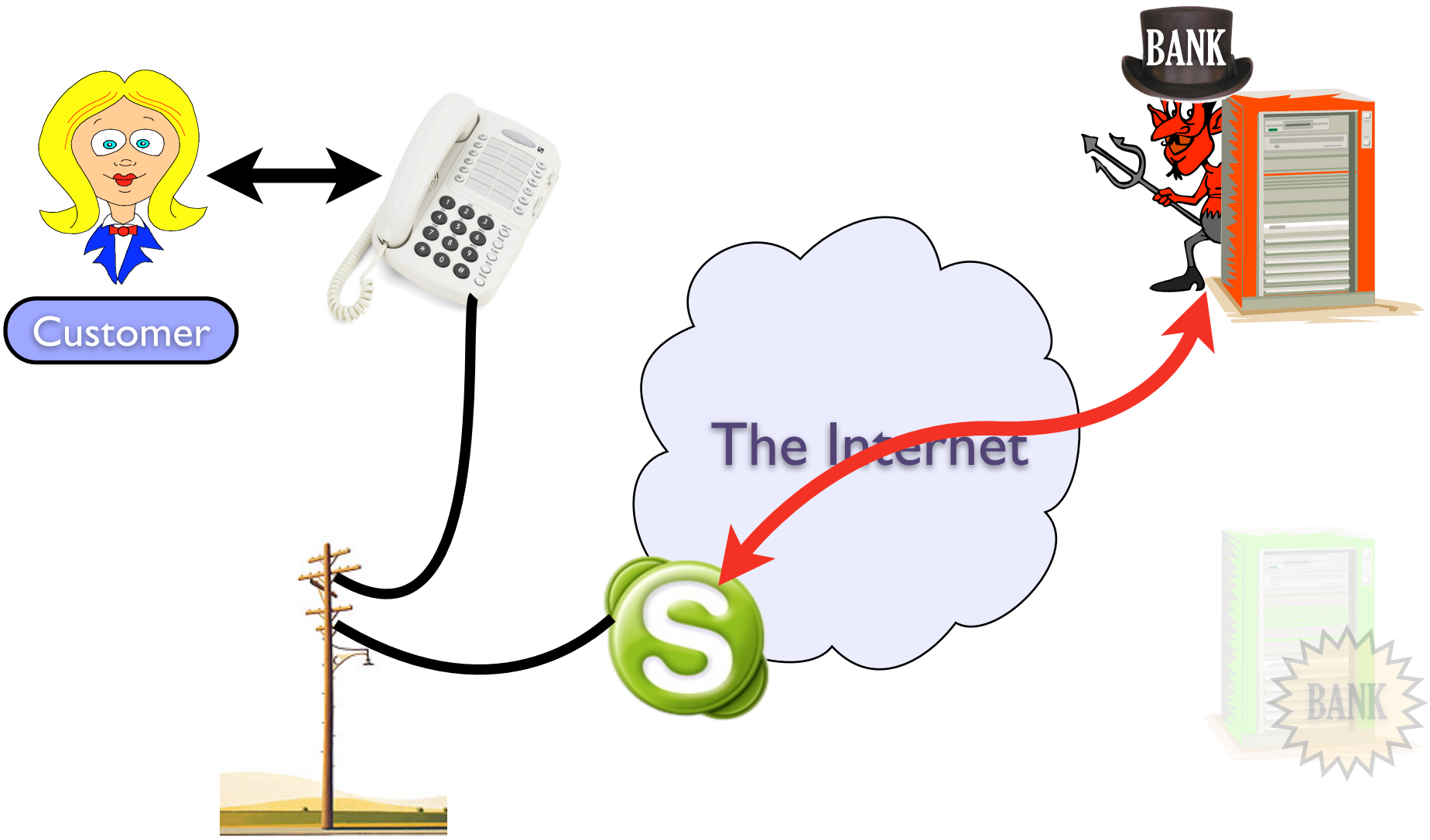
Drive-By Pharming



Drive-By Pharming



Vishing



spoofcard.com (spoof caller id)

Chameleomail

Urgent Message from Your bank

Delete Junk Reply Reply All Forward Print

Dear Customer,

We've noticed some suspicious activity on your account. Please take the time to log into your account and verify your password. To do this, click below:

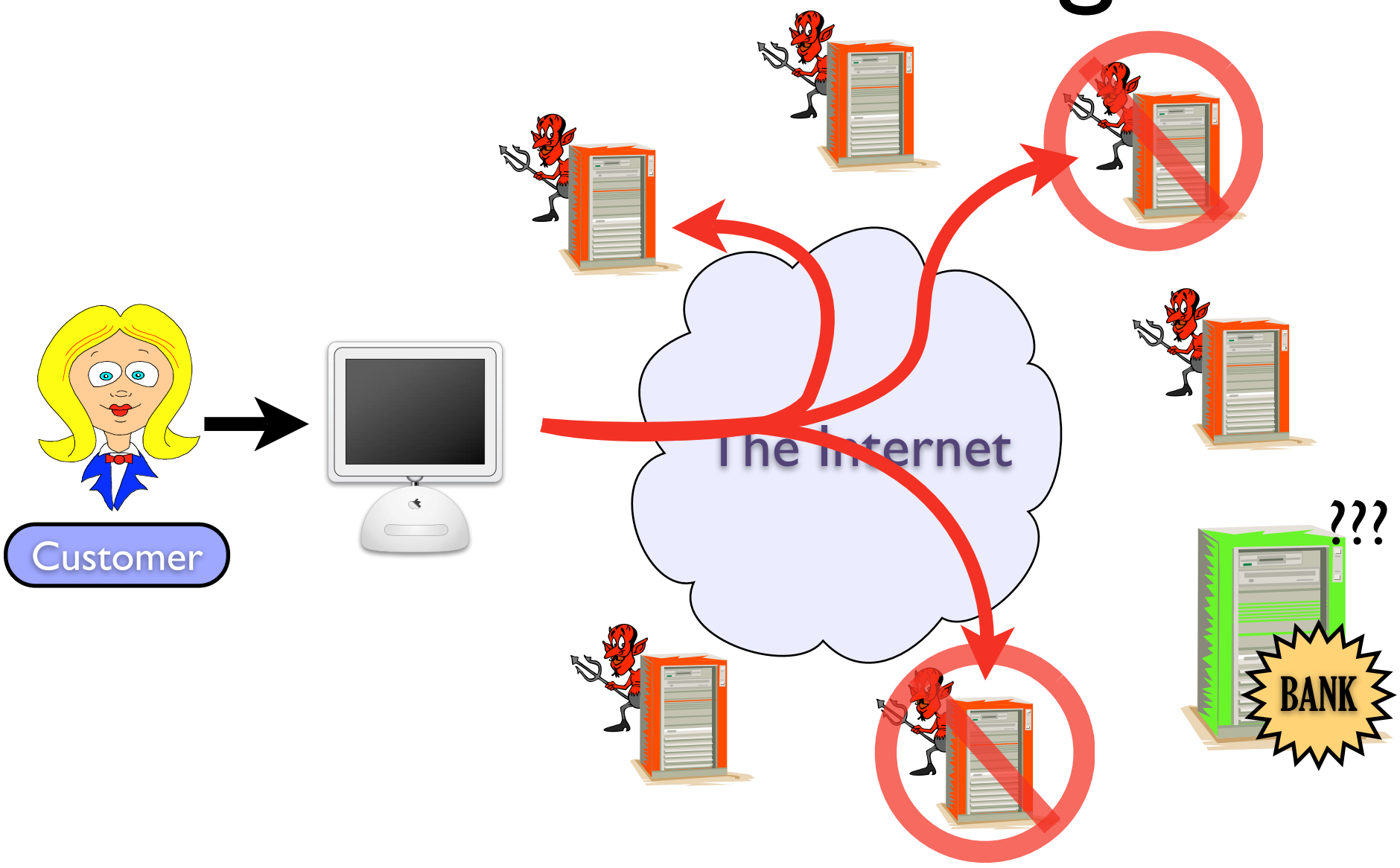
http://www.yourbank.com/phish/login/

Regards,
Your bank

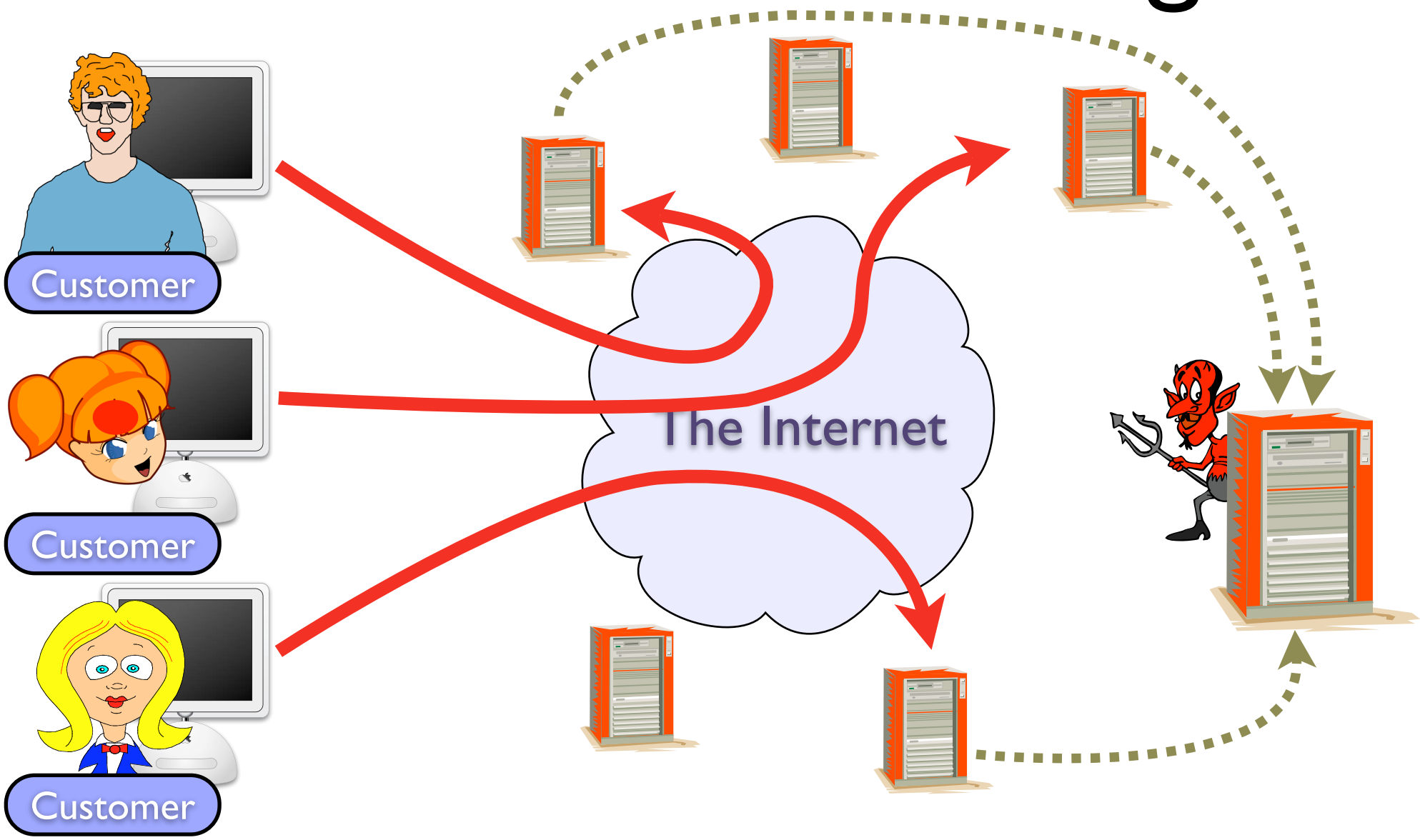
Rock Phishing

http://en.wikipedia.org/wiki/Rock_Phish

Rock Phishing



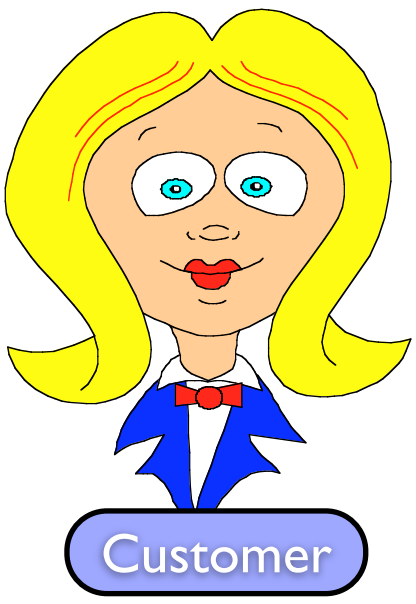
Distributed Phishing



http://eprint.iacr.org/2005/091.pdf

Each victim is pointed to a unique site (a la bot-net)

The Human Factor

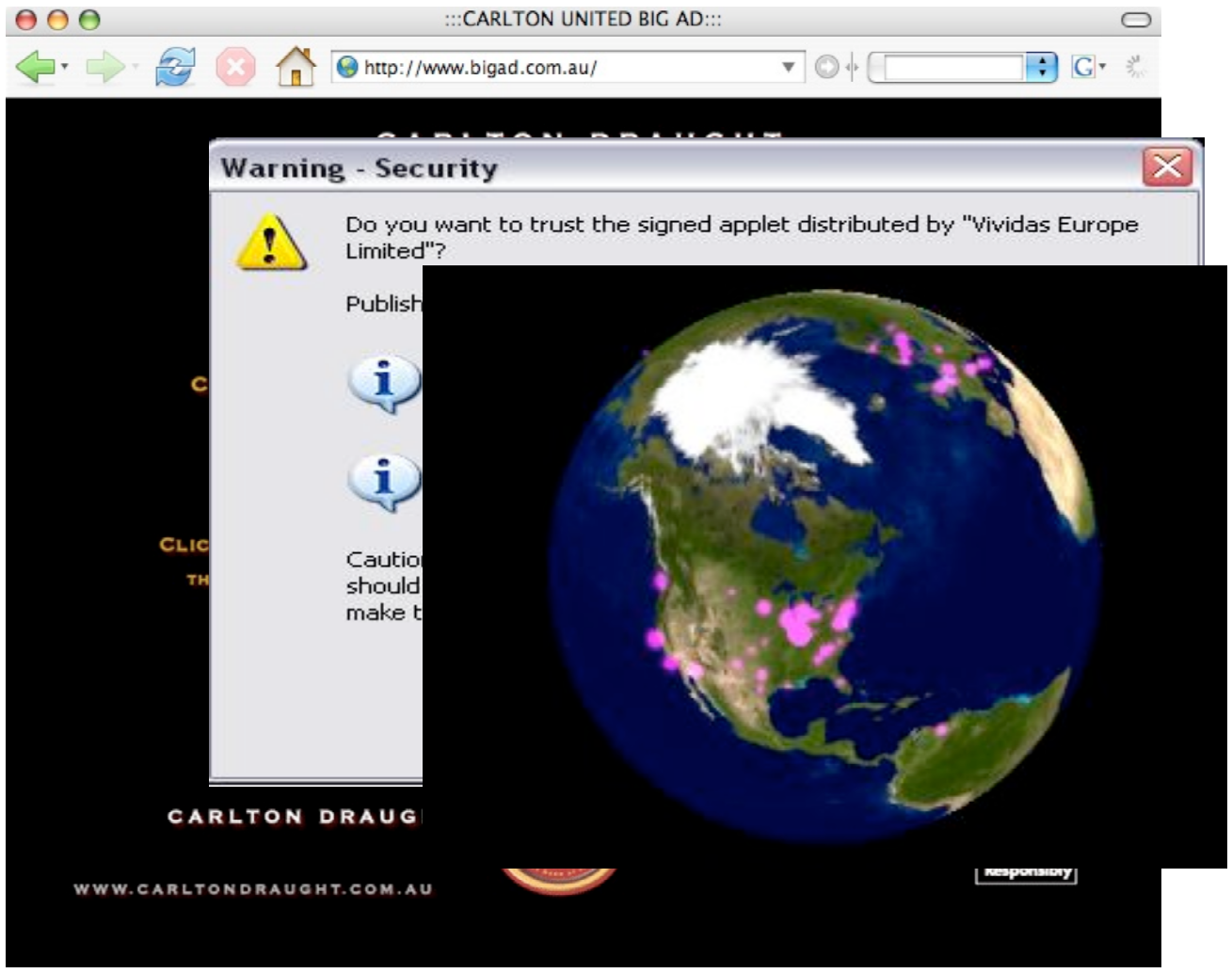


Configuration

http://human-factor.org

Configuration:
- Weak Passwords: Warkitting
- Weak Passwords: Drive-by Pharming

The Human Factor



Neglect

http://human-factor.org

Neglect:
- socially transmitted malware (the security warnings that show up are neglected)

The Human Factor

Deceit

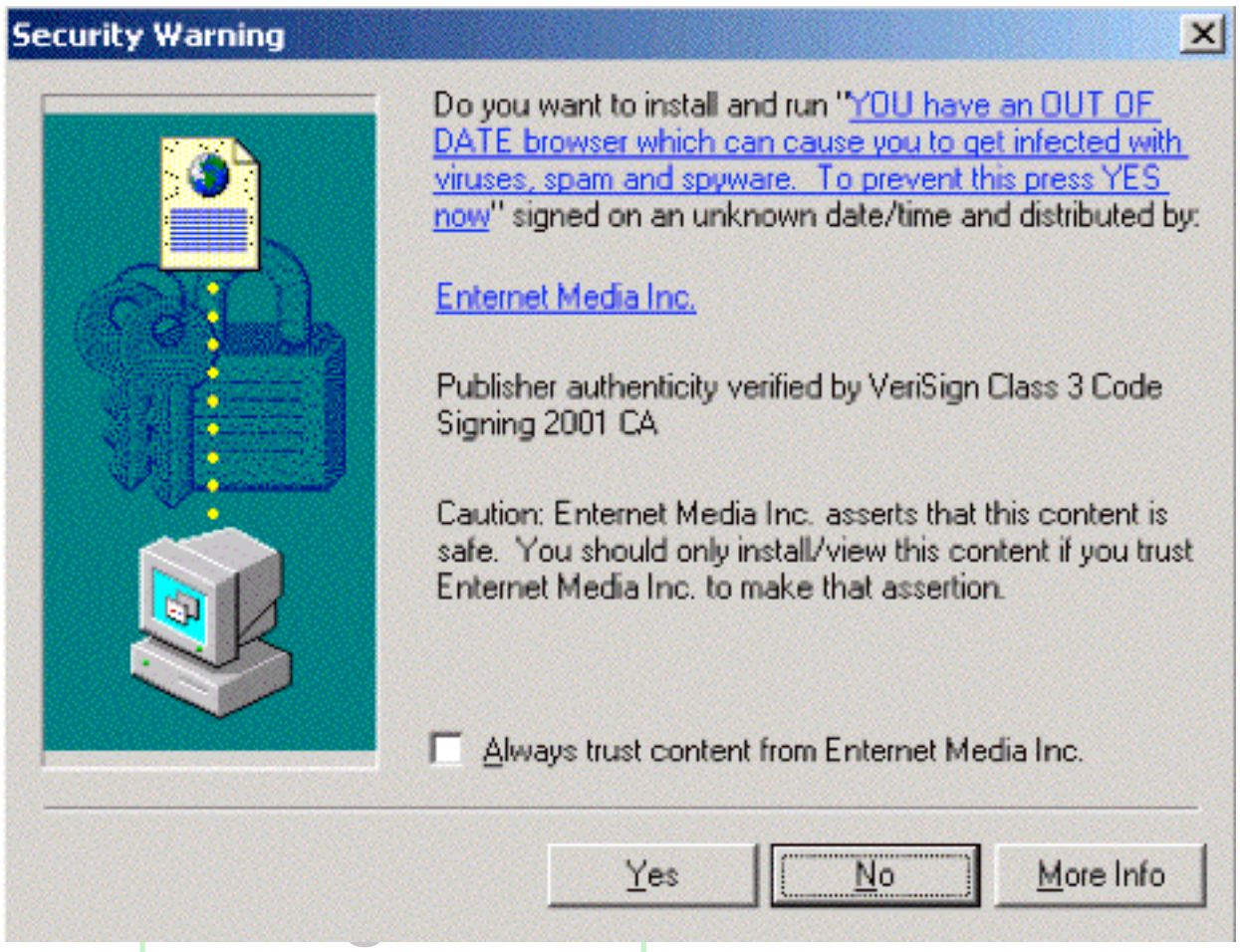
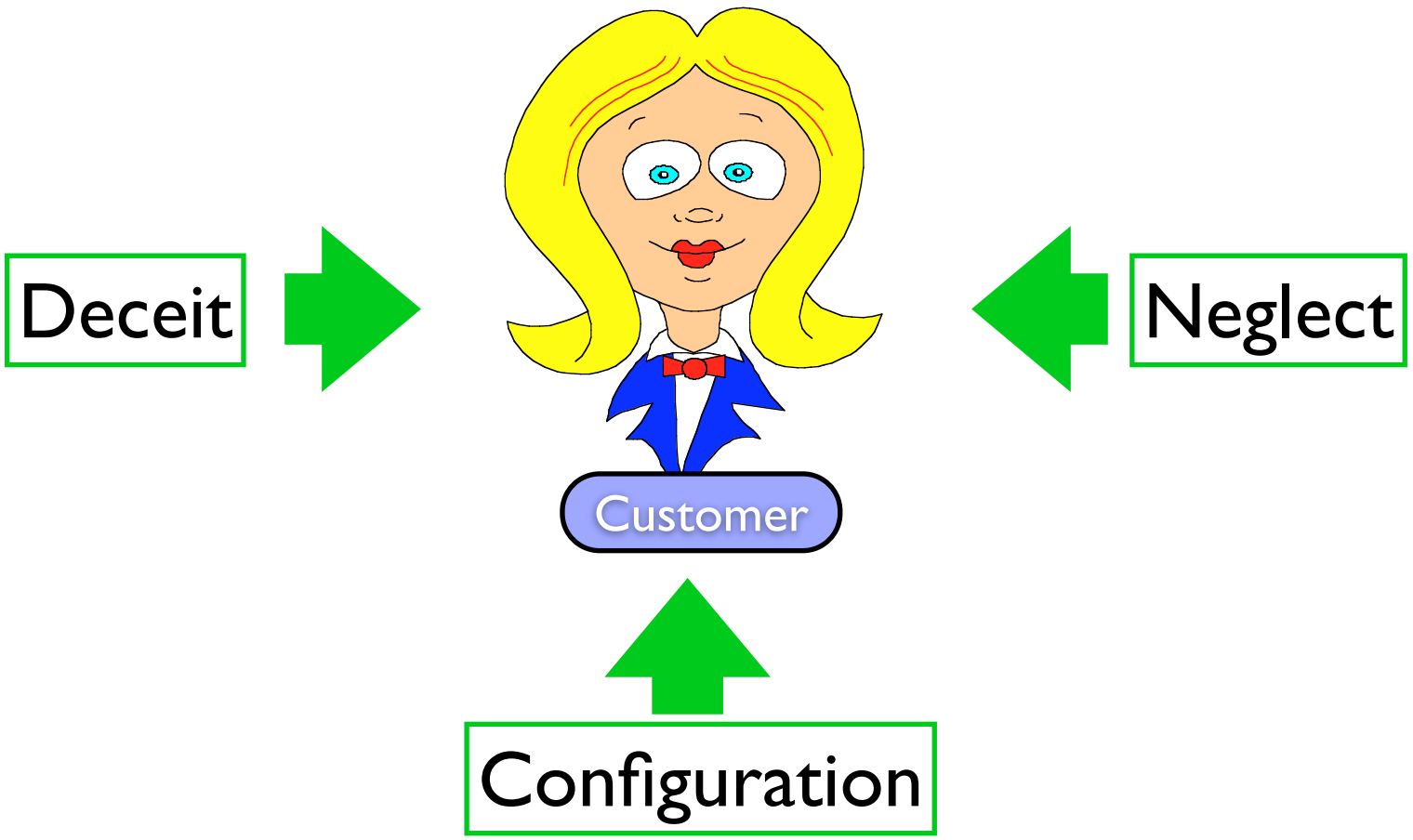


image credit: Ben Edelman

http://human-factor.org

Deceit:
- Do you want to install and run.... “YOU ARE OUT OF DATE, CLICK YES TO PATCH!”
- Social Phishing (social net project)

The Human Factor



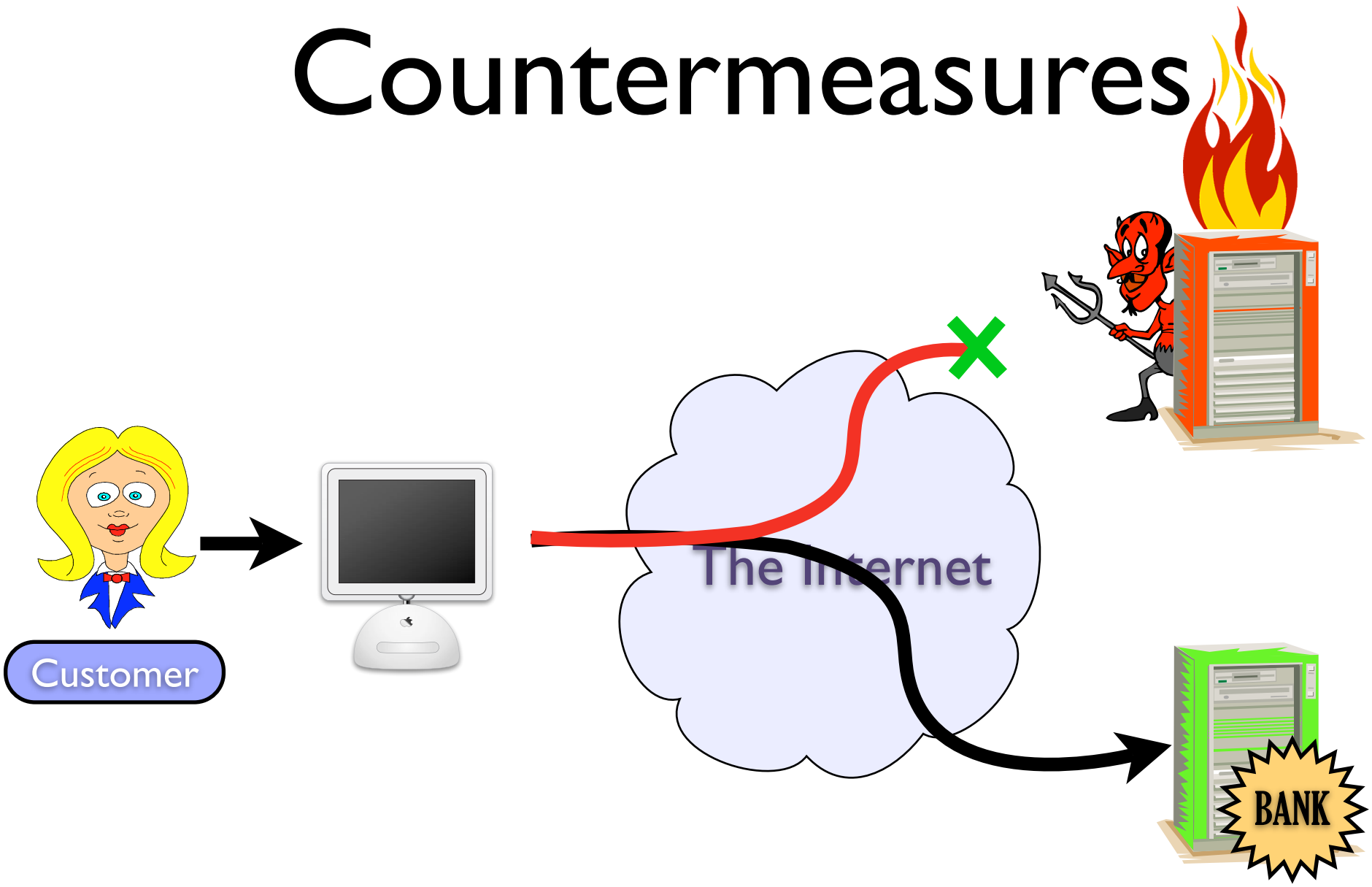
http://human-factor.org

This is what scares me most about the state of internet and communications security

CORE BELIEF:
- People are people, not machines. Need to measure vulnerabilities in-lab/naturalistically to understand threat and how effective countermeasures may be.
- Lab settings may not properly quantify the threat, need to rely on people's everyday frame of mind. ("How many of you have been victim of a phishing attack?")

WHAT MATTERS:
- Padlocks don't. People ignore these indicators.
- Clean URLs matter (short and concise readable ones)

Countermeasures

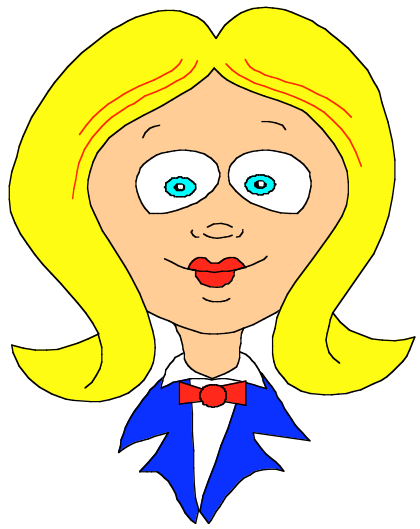


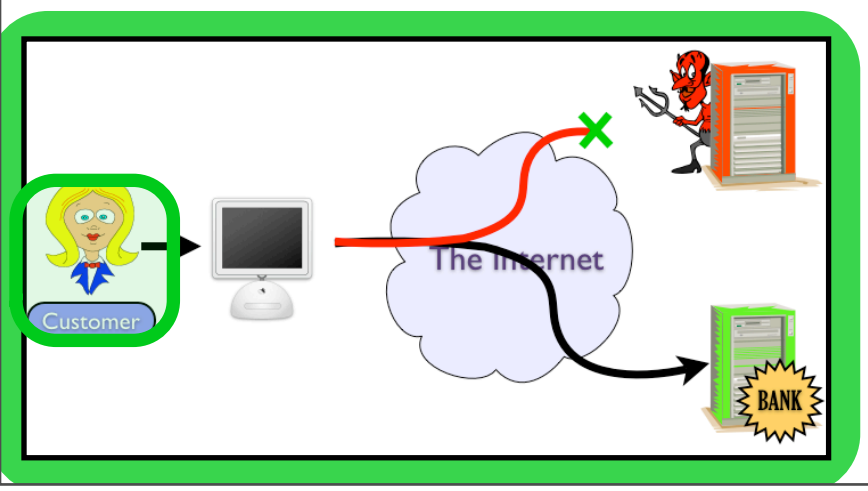
The big question: how do we stop all these strains of attack?

- The problem is not well defined, so solutions are tough to come by
- We are taking an arms-race approach: patching problems one-by-one

SEGWAY: lets see some of the measures that are currently being taken to thwart phishing and pharming... Including those that address the human factor.

Human Education





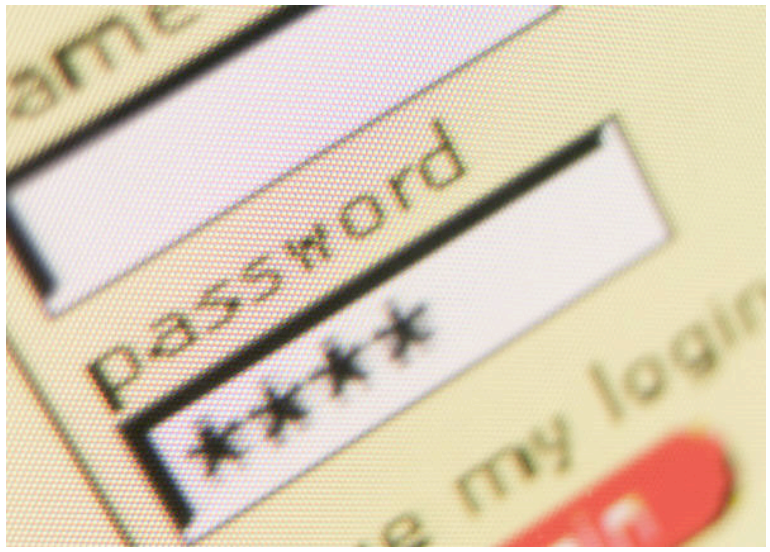
“turn off javascript for trustworthy sites” --> causes people to turn it on to view new Sites (Markus DIMACS report)

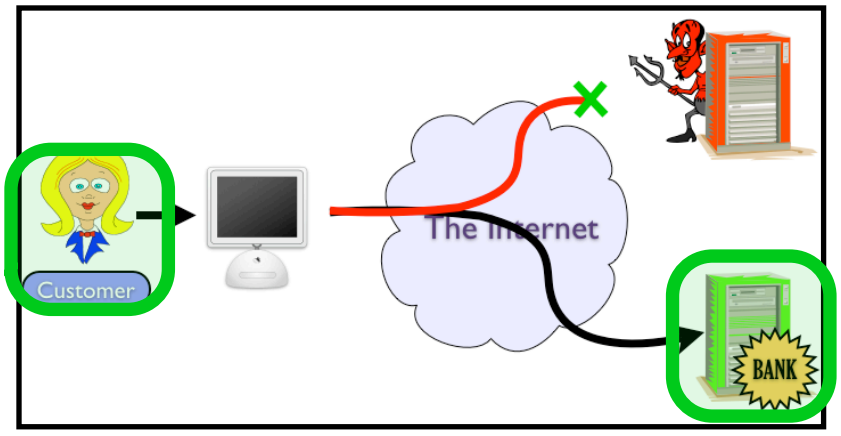
- Alice visits site x (JS off)
- Site x doesn’t load
- Alice gets mad and turns JS on
- Site x loads
- Alice learns to enable JS for all sites.

Another example of where it fails: the padlock (when appearing on the page, not chrome, it is meaningless) -> People misleadingly trust untrustworthy sites.

Two-Factor Authentication

+

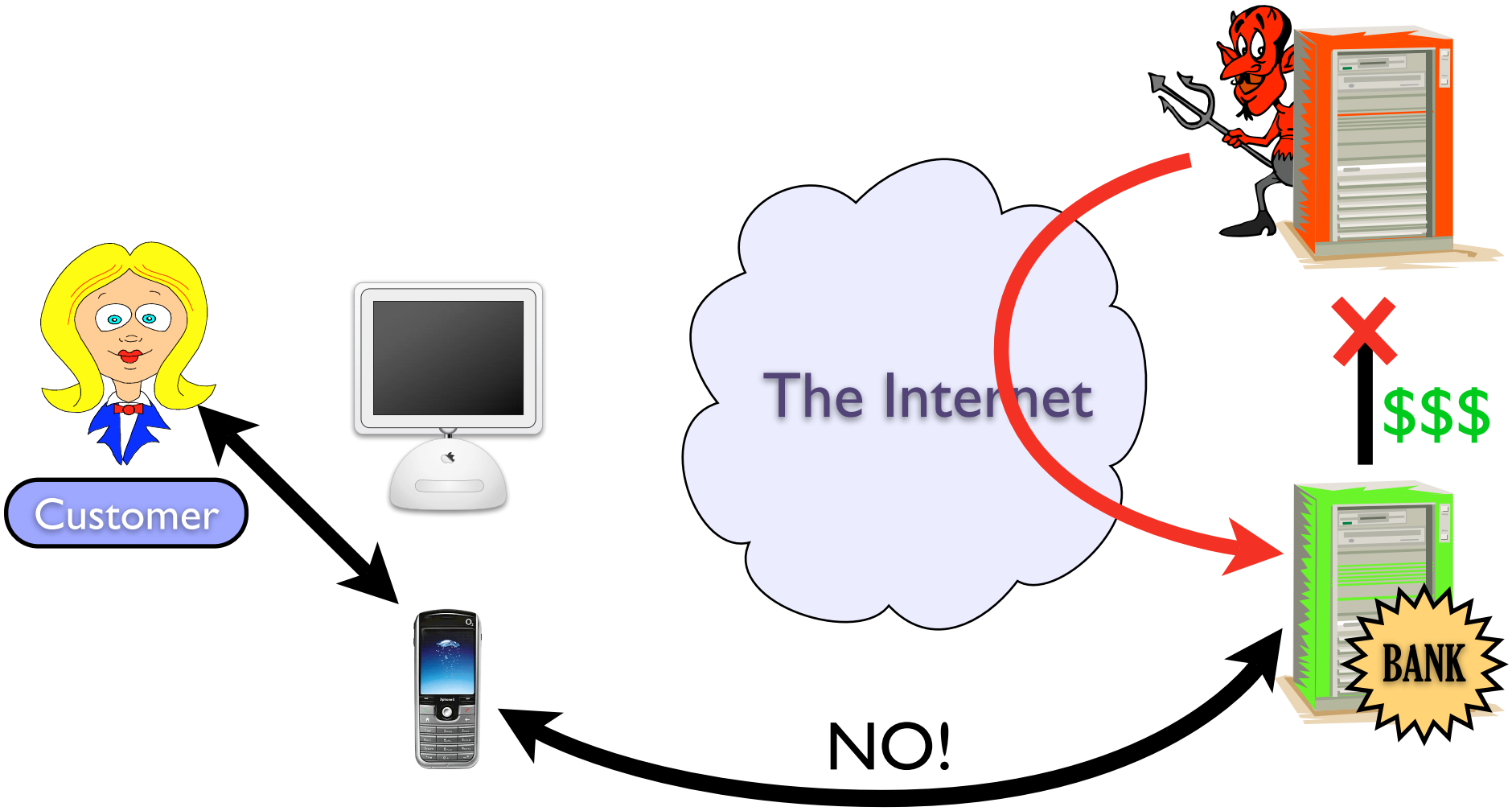




TFA requires more than a password. Sometimes considered two-channel, this is not always the case. Essentially, this requires something besides the password that cannot be easily phished, such as a secure ID (rotating key).

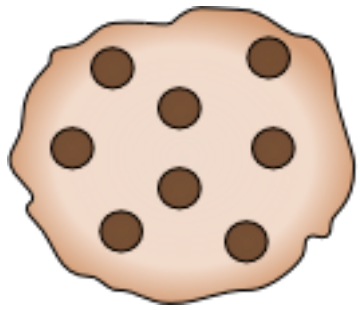
Talk about how some VPNs use crypto tokens with one-time use passwords. This is a weak TFA since it's really just two passwords and the crypto token can more easily be stolen than say a fingerprint -- but fingerprints don't change and can be copied... Thus it's a battle of "what you want".

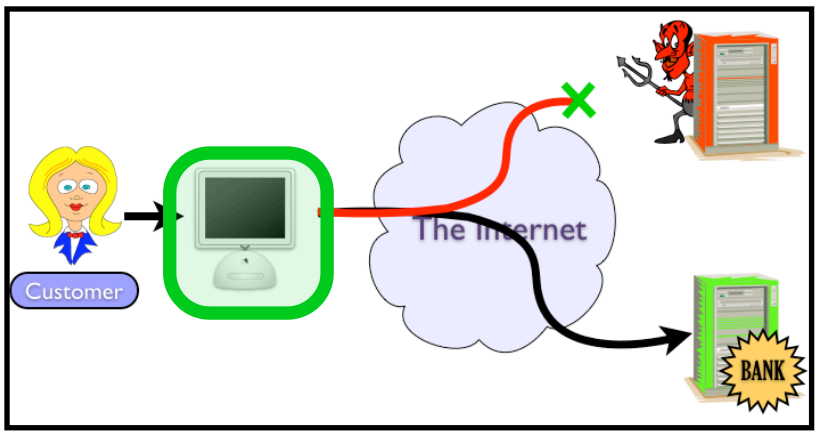
Two-Factor Authentication



This attack fails because the attacker does not have control over the mobile phone. This could be spoofed if the protocol is not properly implemented, however, with spoofcard.com (?) or other caller-id spoofing techniques.

Visitor Cookying





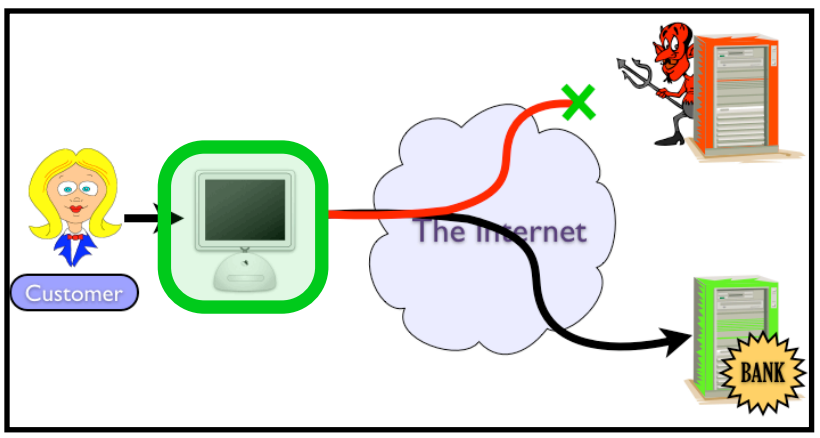
Many institutions have recently implemented this.

- Unrecognized browser visits bank.com,
- the user is asked an extra security question upon login.
- Browser is deemed “trusted” and a cookie is set
- Subsequent visits with the cookie are “trusted”

This is a weak form of TFA, which can be called “sometimes” two-factor.

In my opinion, this can easily be defeated by phishing the security questions, or by more technically advanced cookie-stealing techniques.

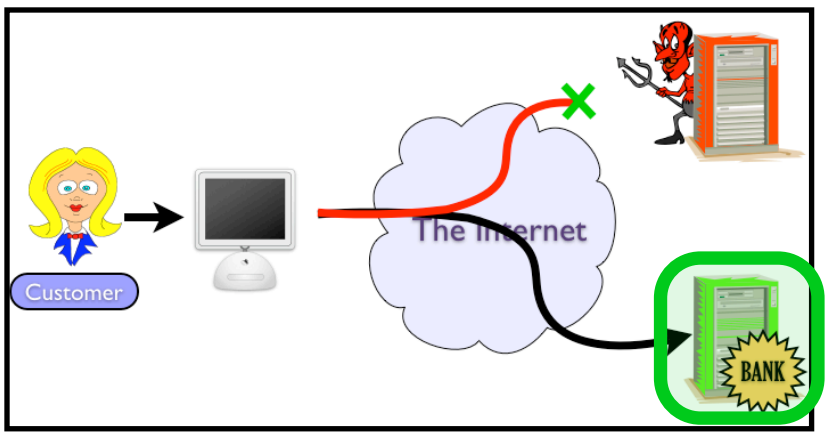
Spam Filter Miracle



What happens if all spam filtering type things work --> we end up with socially transmitted malware (Right people send bad stuff, vishing, etc)

Remote Harm Diagnostics

- ✓ http://www.google.com
- X http://chasebank.some.phisher.com/login.jsp
- X http://207.39.251.3/chasebank.com/login.htm
- X http://j.pmorganchase.com
- ✓ https://jpmorganchase.com
- ✓ http://www.msn.com
- X http://cha5ebank.com/

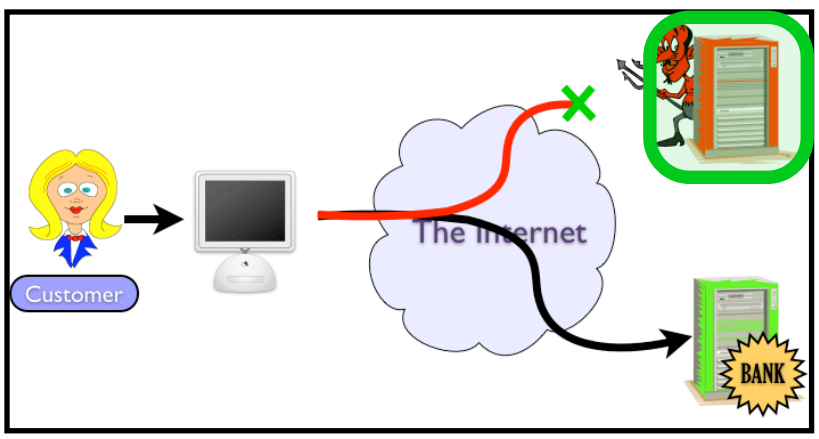


http://ravenwhite.com/whitepapers.html

http://www.darkreading.com/document.asp?doc_id=112797

Same as Chameleomail, but white-hat.

Fast Takedown



Leads to things like distributed phishing, and forces crimeware to perform phishing on the client side.

What's Next?

[[Spend a good amount of time on this slide discussing what might come up in the future]]

1. Phishing blacklists/filters cause -> Fewer "blanket" phishes, more targeted attacks
2. More technically crafty, but widely deployed attacks
   - (advanced rock phish packages)
3. Attacks that rely on the novice user
   - (chameleon emails or websites)
4. Attacks that are driven by new complex web technologies
   - robust JS for making web browsers into bots,
   - maybe some CSS3 tricks to better spoof high-security interfaces
5. Branching out to other sectors, not just financial institutions
6. Attacks that no longer ask for credentials, but money
   - Depends on the willingness of people to pay
   - Harder to prosecute as fraud since the illegality might be fuzzy

SEGWAY: for example, an attack that we're researching right now could occur in the political sector and simply ask for money.

Political Phishing

What good is a judge?
1 message

Howard Dean <democraticparty@politicalphishing.com> **Tue, Jul 03, 2007 at 7:59 PM**
To: csoghoian@gmail.com

THE DEMOCRATIC PARTY

Dear Concerned Citizen,

Yesterday, despite overwhelming public opposition, President Bush commuted the sentence of Scooter Libby, the former White House Chief of Staff to Vice President Cheney who was convicted by a jury of lying about a matter of national security. As yet another example of the elitist attitude that defines Republicans in Washington, he shamelessly put partisan loyalties before the fundamental American value of fair and equal justice under the law.

Bush doesn't care that Libby was convicted by a jury of his peers and sentenced by an experienced federal judge, and he doesn't care that Libby's sentence was well within the sentencing guidelines set by Congress. He once again ignored over 70% of the American public and disregarded the legal process -- this time to help someone who has friends in the right places.

We can't stand for this, and that's why we're doing something to change it. We may not be able to change the President's decision, but we are fighting back -- we're working day and night to take back the White House in 2008 so that we can put an end to just this type of nonsense. Contribute now to help us change things in Washington:

http://www.politicalphishing.com

Source: Christopher Soghoian, http://politicalphishing.com

Banks can be targeted even if banks aren't spoofed. (ACH withdrawals via donations)
Partisan alignment 50% accurate by guessing

Phishing and Pharming

Sid Stamm
Indiana University

What does this all mean?

The arms race is speeding up, and we need to reign it in.

The human factor is ever so important, so we need to address it more strongly -- or more accurately.

- That's one thing we're working on at IU.

Originally phishing and pharming worked because people didn't understand how the internet worked and how web pages operate.

- People were starting to learn, but with Web2.0 and new technologies (like CSS), it just gets harder.