Modern day magic on the Internet

(Social Engineering)

Greg Day
Principal Security Analyst, EMEA

- Q: Social engineering has been around for years, what's changed?

- What are today's common risks from social engineering?
  - Direct users to malware attack
  - Trick users into executing malware
  - Persuade users into handing over information (data leakage)

- Q: Do you invest appropriate time/resources into stopping social engineering?
  - Does your anti-malware solve the problem, or should I be doing more?

A quick recap…

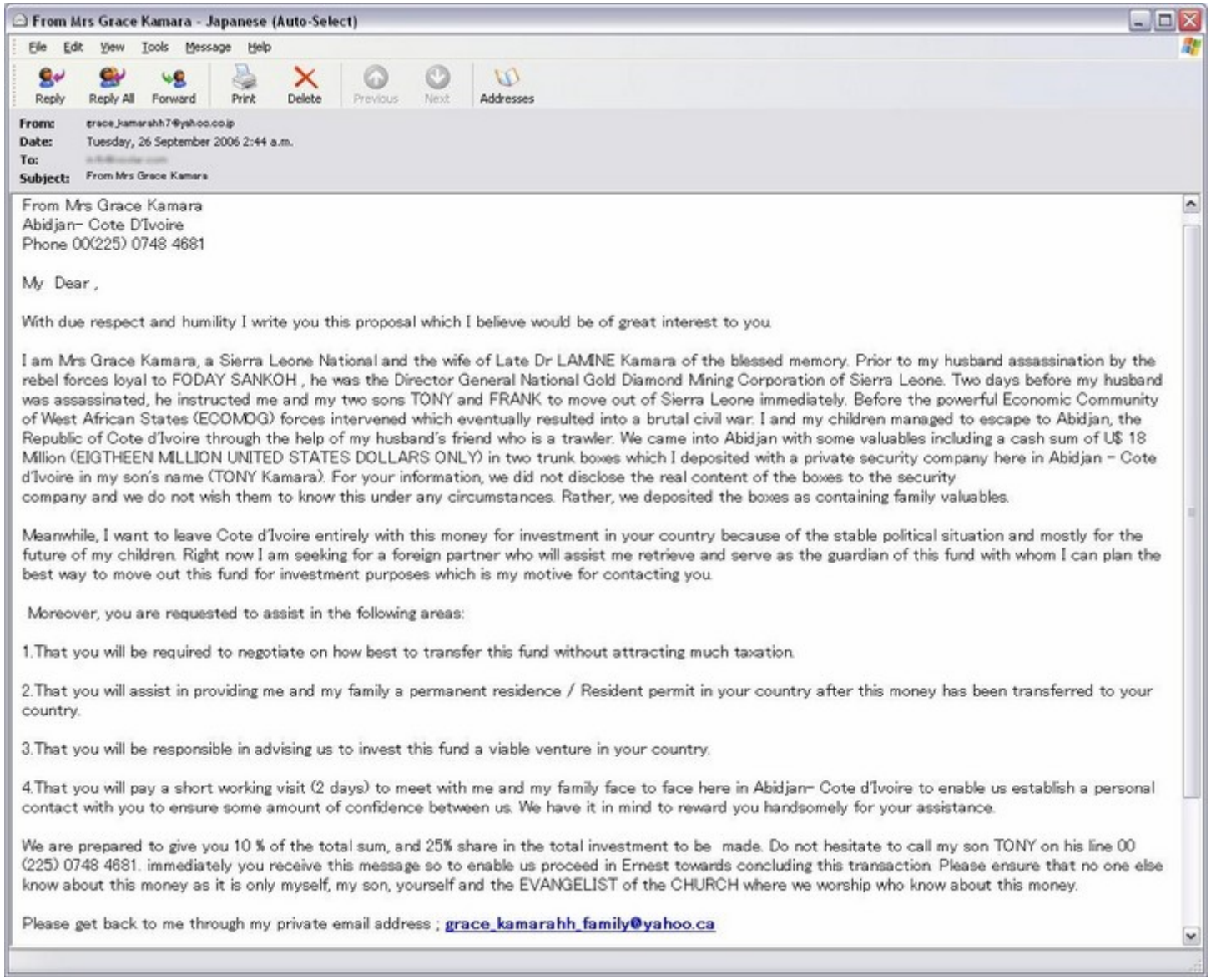
What is social engineering?

- All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases.

- These biases, sometimes called "bugs in the human hardware," are exploited in various combinations to create attack techniques

Source: http://en.wikipedia.org/wiki/Social_engineering_(security)

Nigeria 419 scams – since 1980's



From Mrs Grace Kamara - Japanese (Auto-Select)

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: grace_kamarahh7@yahoo.co.jp
Date: Tuesday, 26 September 2006 2:44 a.m.
To:
Subject: From Mrs Grace Kamara

From Mrs Grace Kamara
Abidjan– Cote D'Ivoire
Phone 00(225) 0748 4681

My Dear ,

With due respect and humility I write you this proposal which I believe would be of great interest to you.

I am Mrs Grace Kamara, a Sierra Leone National and the wife of Late Dr LAMINE Kamara of the blessed memory. Prior to my husband assassination by the rebel forces loyal to FODAY SANKOH , he was the Director General National Gold Diamond Mining Corporation of Sierra Leone. Two days before my husband was assassinated, he instructed me and my two sons TONY and FRANK to move out of Sierra Leone immediately. Before the powerful Economic Community of West African States (ECOMOG) forces intervened which eventually resulted into a brutal civil war. I and my children managed to escape to Abidjan, the Republic of Cote d'Ivoire through the help of my husband's friend who is a trawler. We came into Abidjan with some valuables including a cash sum of U$ 18 Million (EIGTHEEN MILLION UNITED STATES DOLLARS ONLY) in two trunk boxes which I deposited with a private security company here in Abidjan – Cote d'Ivoire in my son's name (TONY Kamara). For your information, we did not disclose the real content of the boxes to the security company and we do not wish them to know this under any circumstances. Rather, we deposited the boxes as containing family valuables.

Meanwhile, I want to leave Cote d'Ivoire entirely with this money for investment in your country because of the stable political situation and mostly for the future of my children. Right now I am seeking for a foreign partner who will assist me retrieve and serve as the guardian of this fund with whom I can plan the best way to move out this fund for investment purposes which is my motive for contacting you.

Moreover, you are requested to assist in the following areas:

1.That you will be required to negotiate on how best to transfer this fund without attracting much taxation.

2.That you will assist in providing me and my family a permanent residence / Resident permit in your country after this money has been transferred to your country.

3.That you will be responsible in advising us to invest this fund a viable venture in your country.

4.That you will pay a short working visit (2 days) to meet with me and my family face to face here in Abidjan– Cote d'Ivoire to enable us establish a personal contact with you to ensure some amount of confidence between us. We have it in mind to reward you handsomely for your assistance.

We are prepared to give you 10 % of the total sum, and 25% share in the total investment to be made. Do not hesitate to call my son TONY on his line 00 (225) 0748 4681. immediately you receive this message so to enable us proceed in Ernest towards concluding this transaction. Please ensure that no one else know about this money as it is only myself, my son, yourself and the EVANGELIST of the CHURCH where we worship who know about this money.

Please get back to me through my private email address ; grace_kamarahh_family@yahoo.ca

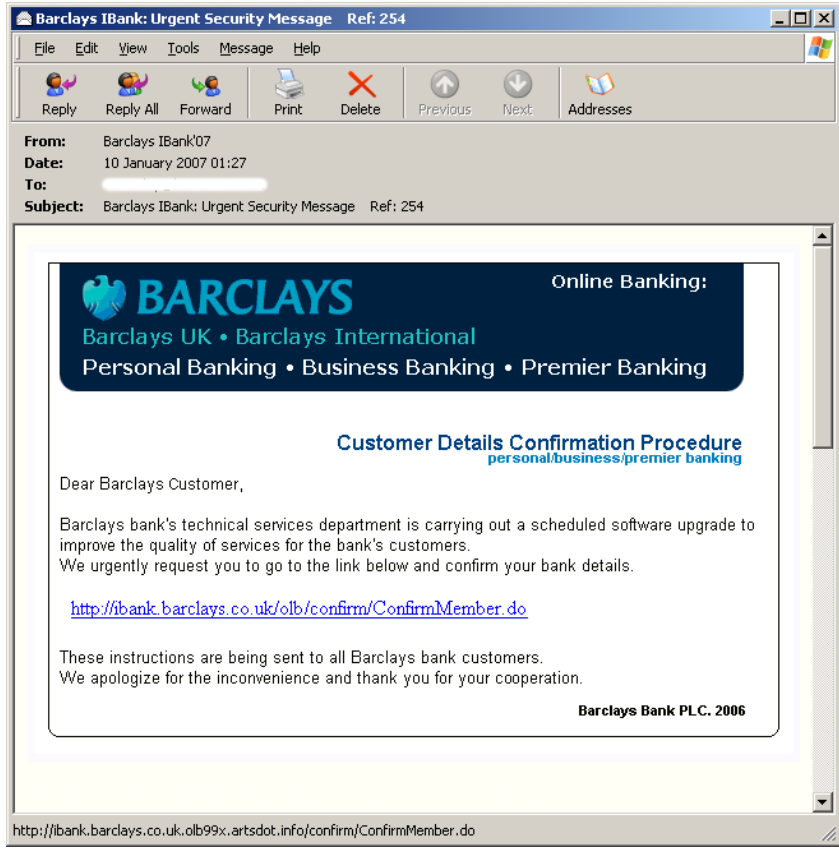
Early Phishing….Wolves on AOL

- AOL's chat rooms have been awash in password-stealing since at least 1994 Salon.com
- In one three-month period in 1996, AOL cancelled 370,000 accounts for "credit card fraud, hacking, etc.“ Washington post
- Steve Case's (Co-founder & CEO of AOL), April 1996 letter to all members

> “…you may have noticed that we recently added new "alert" text on the Instant Message and e-mail forms reading: "Reminder: AOL Staff will never ask for your password or billing information :-)."
>
> This is the first in a series of efforts we will roll out over the next few months to [attempt to] put an end to ***"password fishing" -- the practice where computer hackers prey on new users by impersonating AOL staff and soliciting passwords and credit card information***.”
>
> ...certain individuals try to take advantage of others. Since our community has more than 5 million members, it's like a large city, so we have to [try to] take action together to put an end to inappropriate or illegal behavior.
>
> ***Remember my monthly motto: Do not give out your password to anyone, whether it's online or even on the phone.***

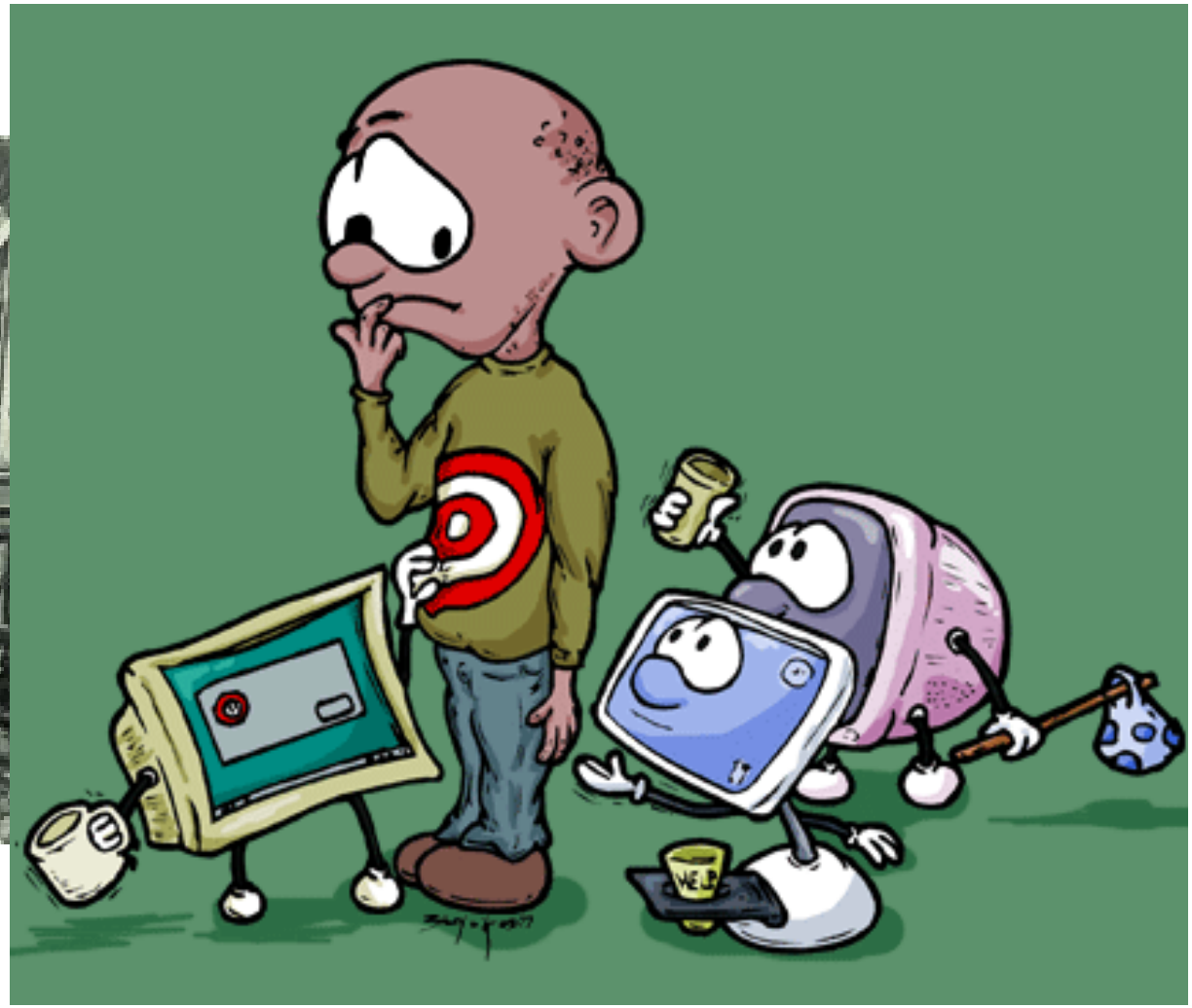
Source: http://www.aolwatch.org/speaks.htm

Emails – Since the 90's

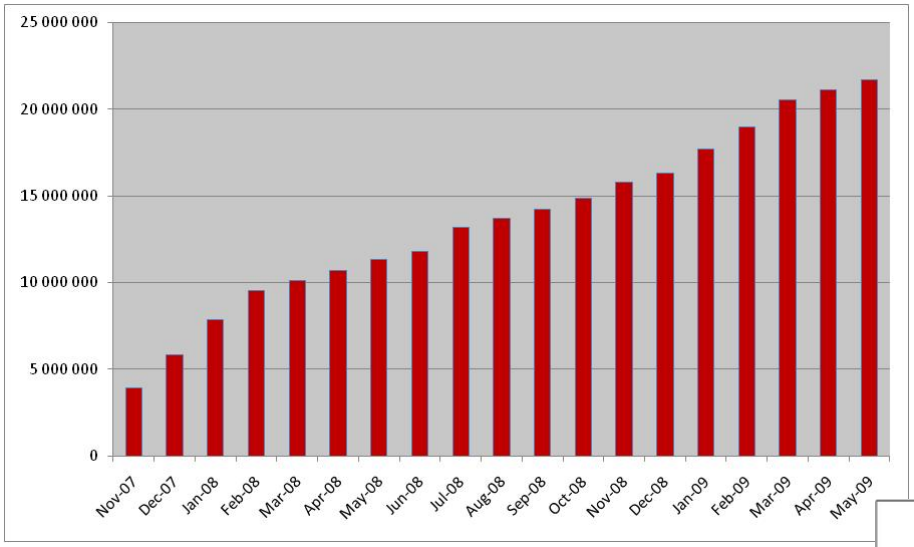


So what’s changed?

No more great train robberies – Little & often

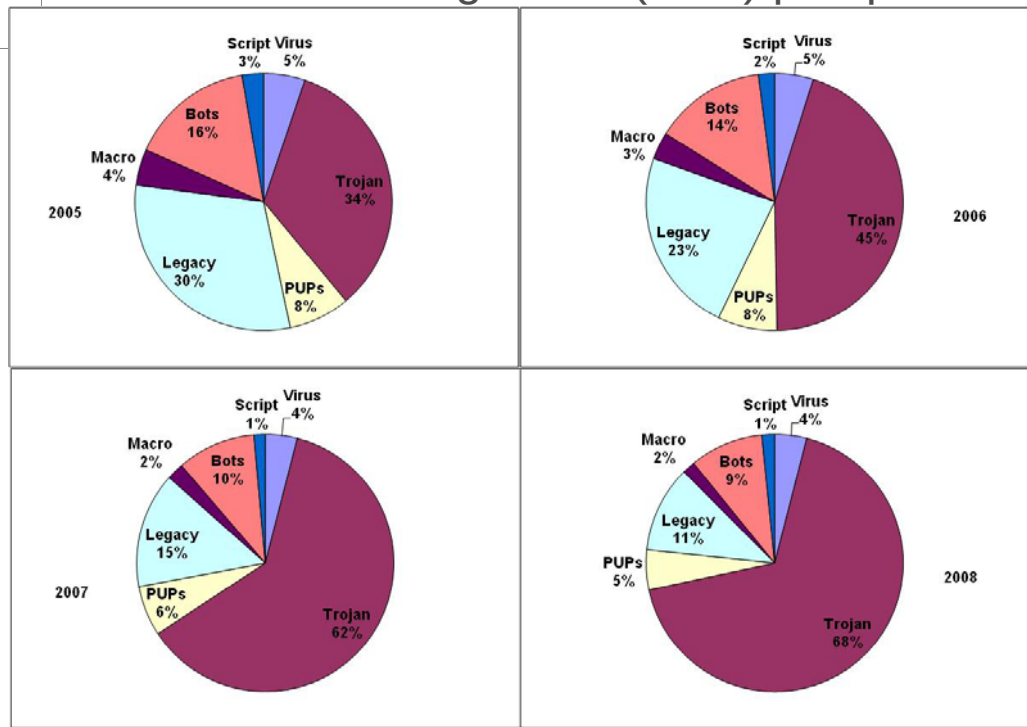


The changing face of Malware

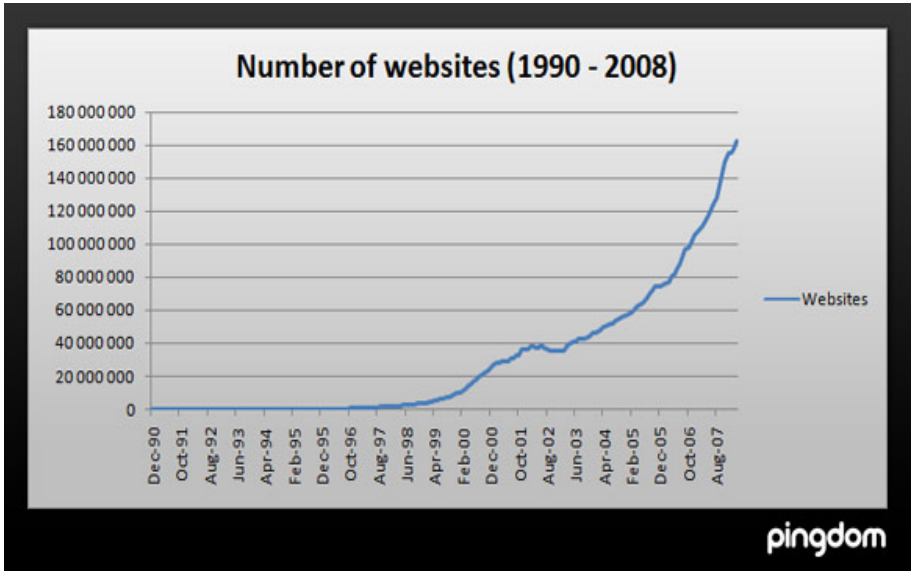


McAfee known malware (zoo) count

Distribution from signature (DAT) perspective



Trojans can get lost in the volume of the Web



The graph covers December 1990 to March 2008.

Online presence

1,463,632,361 – Internet users worldwide (June 2008).

Email

- **1.3 billion** – email users worldwide.
- **210 billion** – emails sent per day (2008)

Web Sites

- **186,727,854** – in December 2008.
- **31.5 million** – added during 2008.

Source: http://royal.pingdom.com/2009/01/22/internet-2008-in-numbers/

Graph source: http://royal.pingdom.com/2008/04/04/how-we-got-from-1-to-162-million-websites-on-the-internet/

Social engineering misdirection

- Misdirection takes advantage of the limits of the human mind in order to give the wrong picture and memory. The mind can concentrate on only one thing at a time. The magician uses this to manipulate the "victim's" idea of how the world is supposed to be.

Source: http://en.wikipedia.org/wiki/Misdirection_(magic)

Thimblerig game

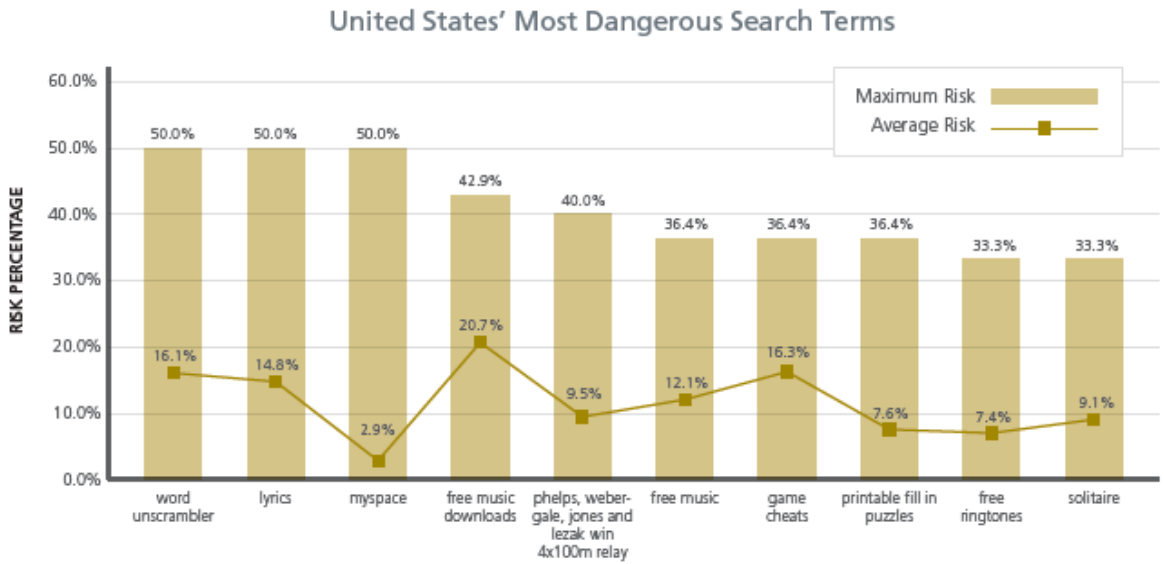
1670 (Hull Elections - Richard Perry and his fiddler wife)

How to get users to your attack

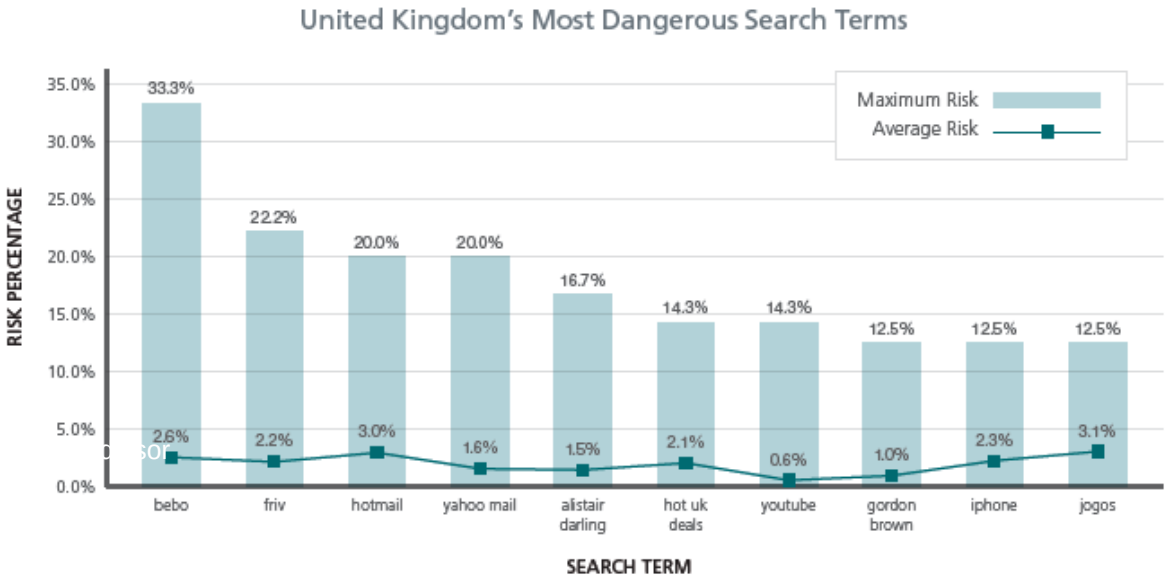
Finger on the pulse of what's hip and cool (popular)

McAfee

North America



- Election 08
- Shopping
- How Do I?
- Astrology
- Sports
- Destinations
- Health
- Economic Crisis



Using celebrities popularity

	2007	2008	US 2009 (Risk %)	UK 2009 (Risk %)
1	Paris Hilton	Brad Pitt	Jessica Biel (20.1)	Katie Price (16.3)
2	Amy Winehouse	Beyonce	Beyonce (17.9)	Jude Law (15.4)
3	Cristiano Ronaldo	Justin Timberlake	Tom Brady (17.4)	Victoria Beckham (13.6)
4	Britney Spears	Heidi Montag	Jessica Simpson (17.6)	Kate Moss (12.6)
5	Heidi Klum	Mariah Carey	Jennifer Aniston (12.3)	David Beckham (12.1)
6	Peter Doherty & Valentino Rossi	Jessica Alba	Gisele Bundchen (15.8)	Daniel Radcliffe (12)
7	Jose Mourinho	Lindsey Lohan	Miley Cyrus (15.5)	Kerry Katona (9)
8	Madeleine Bernadotte	Cameron Diaz	Megan Fox (15.3) & Angelina Jolie (15.3)	Amy Winehouse (8.6)
9	Charlize Theron, Elisabetta Canalis & Nicolas Sarkozy	George Clooney & Rihanna	Ashley Tidsdale (14.9)	Cheryl Cole (8.5)
10	Antonio Banderas	Angelina Jolie	Brad Pitt (14.8)	Leona Lewis (8.3)
11			Reece Witherspoon (14.4)	Daniel Craig (8.1)
12			Britney Spears (14.3)	Lilly Allen (7.4)
13			Rihanna (14.1)	Sadie Frost (6.7)
14			Lindsay Lohan (14)	Peter Andre (6.2) & Prince Harry (6.2)
15			Kim Kardashian (13.8)	Wayne Rooney (4.8)

Source: McAfee SiteAdvisor

Paris Hilton Examples

McAfee

Paris Hilt
31 Jul 2009
Paris Hilto
www.popcru
quest/ - Cac

popcrunch.com

When we browsed this site, it made unauthorized changes to our test PC.

Are you the owner of this site? Leave a comment

Contact information:

Popularity

Lots of users

AUTOMATED WEB SAFETY TESTING RESULTS FOR POPCRUNCH.COM

BROWSER EXPLOIT:

Breached browser security

When we browsed this site, it made unauthorized changes to our test PC.

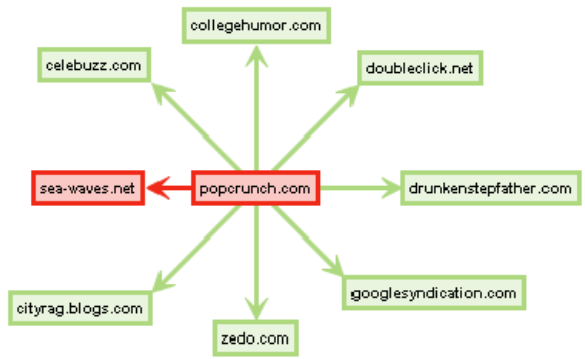
E-MAIL TESTS FOR POPCRUNCH.COM:

DOWNLOAD TESTS FOR POPCRUNCH.COM:

ONLINE AFFILIATIONS FOR POPCRUNCH.COM:

Linked to green sites

When we visited this site, we found that most of its links are to sites which are safe or have only minor safety/annoyance issues.



ANNOYANCES FROM POPCRUNCH.COM:

Third-Party Cookies

burstnet.com

If it's making headlines, cyber attackers will start their social engineering: Swine Flu

McAfee

REUTERS

LATEST NEWS U.S. TO WORK WITH GM AHEAD OF JUNE 1 DEADLINE

Top News
Reuters top ten news stories delivered to your inbox each day.
Subscribe

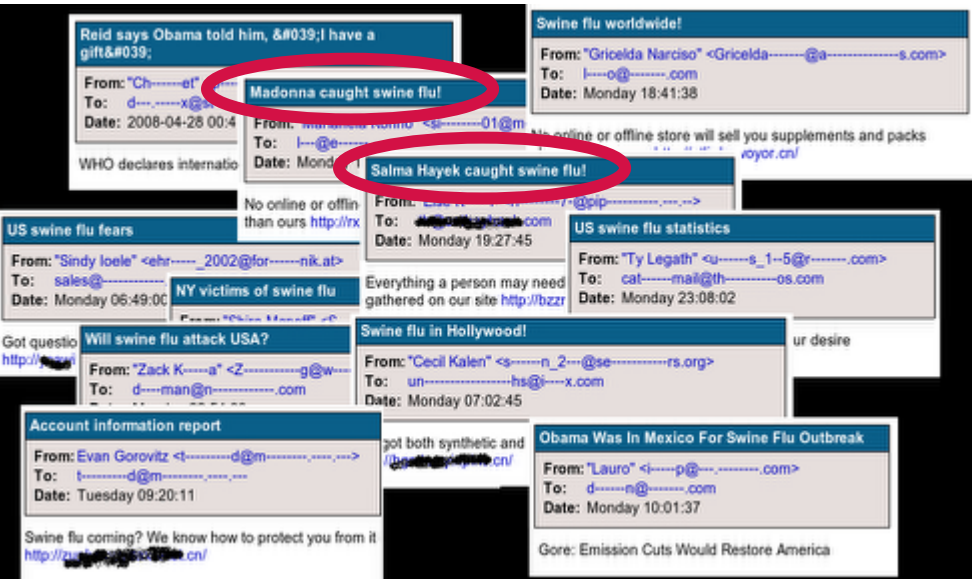
Start Trading With ONLY $25

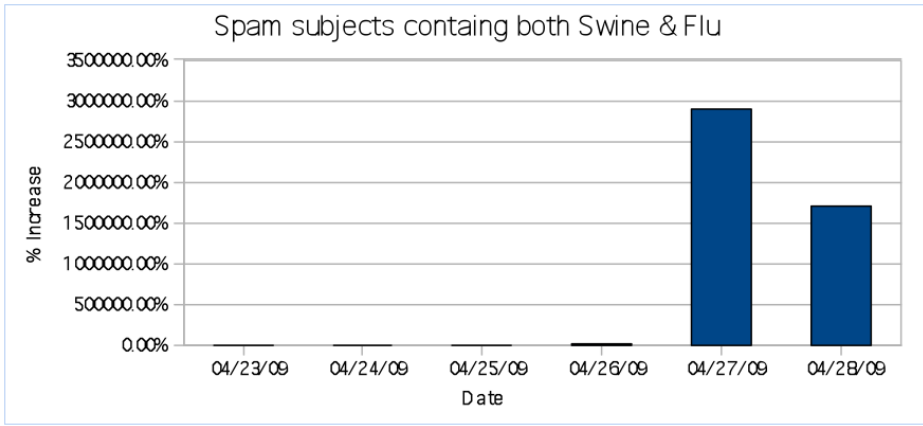
You are here: Home > News > International > Article

HOME
BUSINESS & FINANCE
NEWS
U.S.

New, deadly swine flu hits Mexico, may spread

Fri Apr 24, 2009 11:22am EDT

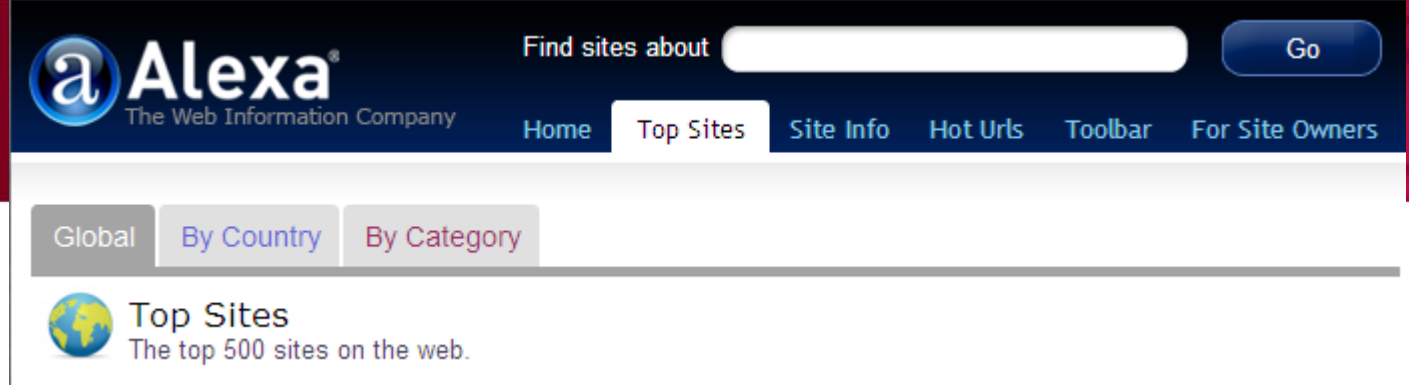




Social networking – A route to victim

Cyber attackers use Terrorist tactics
- Hubs on online users (social networking)

- “…. terrorist cells are increasingly looking at less well-protected "soft" targets where Westerners can be found, such as social and retail venues, tourist sites and transport networks (rail, road and airports), as illustrated by the attacks in Bali in October 2002, Madrid in March 2004 and Egypt in July 2005.”



McAfee

1. **Google** (google.com) - Enables users to search the Web, Usenet, and images. Features include PageRank, caching and translation of results, and an option to find similar pages. The company's focus is developing search technology.
2. **Yahoo** (yahoo.com) - Personalized content and search options. Chatrooms, free e-mail, clubs, and pager.
3. **Facebook** (facebook.com) - A social utility that connects people to keep up with friends, upload photos, share links and videos.
4. **YouTube** (youtube.com) - YouTube is a way to get your videos to the people who matter to you. Upload, tag and share your videos worldwide!
5. **Windows Live** (live.com) - Search engine from Microsoft.
6. **Wikipedia** (wikipedia.org) - An online collaborative encyclopedia.
7. **Blogger** (blogger.com) - Free, automated weblog publishing tool that sends updates to a site via FTP.
8. **Microsoft Network (MSN)** (msn.com) - Dialup access and content provider.
9. **Yahoo!カテゴリ** (yahoo.co.jp) - 有料審査制のディレクトリ。ウェブサービスの形でAPIを公開。
10. **Baidu.com** (baidu.com) - The leading Chinese language search engine, provides "simple and reliable" search experience, strong in Chinese language and multi-media content including MP3 music and movies, the first to offer WAP and PDA-based mobile search in China.
11. **Myspace** (myspace.com) - Social Networking Site.
12. **Google India** (google.co.in) - Indian version of this popular search engine. Search the whole web or only webpages from India. Interfaces offered in English, Hindi, Bengali, Telugu, Marathi and Tamil.
13. **Google** (google.de) - Suche im gesamten Web, in deutschsprachigen sowie in deutschen Seiten. Zusätzlich ist eine Bildersuche, eine Newsarchiv-Suche (ehemals dejanews) sowie ein Katalog vorhanden.
14. **Twitter** (twitter.com) - Social networking and microblogging service utilising instant messaging, SMS or a web interface.
15. **QQ.COM** (qq.com) - 中国最大的门户网站，提供即时通讯、新闻资讯、网络游戏以及在线拍卖业务

But what people do at home it there own problem! Facebook - Just how much business time?

77% of employees have a Facebook account

⅔rd access during working hours for average 15mins per day

87% couldn't define a clear business reason

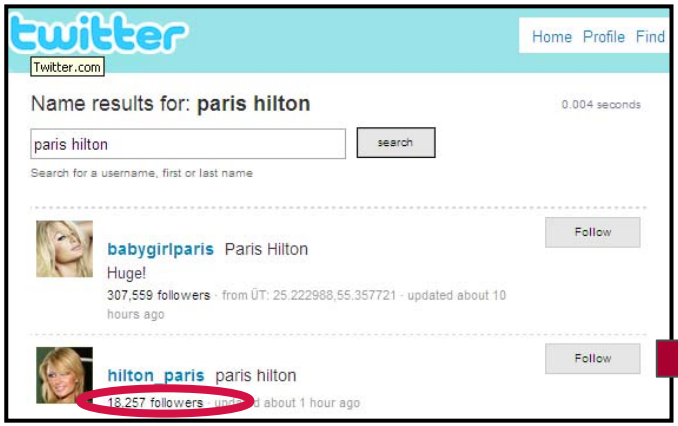
1 in 33 built and manage their entire profile at work

1.47% total lost productivity across entire employee population

Source: http://nucleusresearch.com/research/notes-and-reports/facebook-measuring-the-cost-to-business-of-social-notworking/

Common issues with social networking

- Who are you really communicating with?



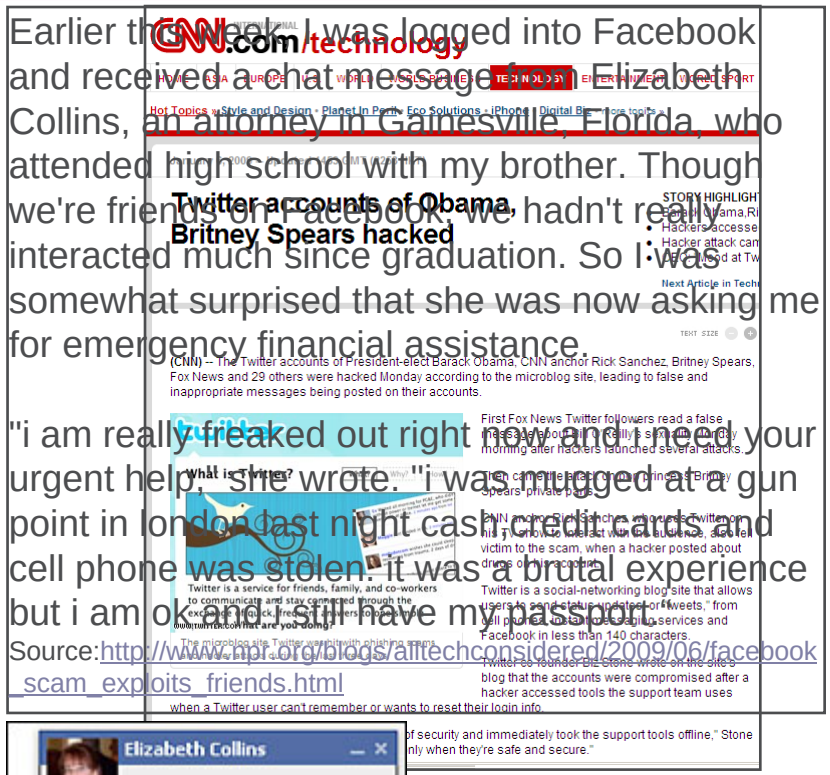
Common issues with social networking

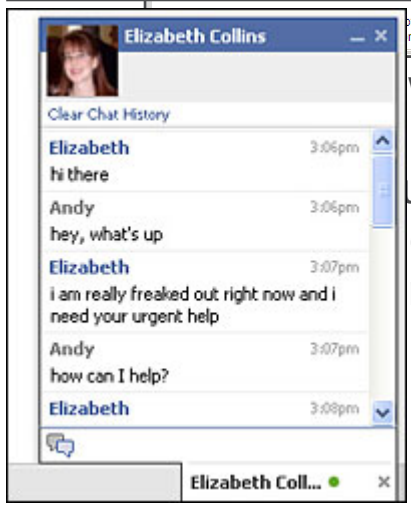
- Who are you really communicating with?
  - Has their account been compromised?
  - Has the provider of the tool/service been compromised?

Earlier this week I was logged into Facebook and received a chat message from Elizabeth Collins, an attorney in Gainesville, Florida, who attended high school with my brother. Though we're friends on Facebook, we hadn't really interacted much since graduation. So I was somewhat surprised that she was now asking me for emergency financial assistance.

"i am really freaked out right now and need your urgent help," she wrote. "i was mugged at a gun point in london last night cash,credit,cards and cell phone was stolen. it was a brutal experience but i am ok and still have my passport.

Source:http://www.npr.org/blogs/alltechconsidered/2009/06/facebook_scam_exploits_friends.html





were compromised
accessed tools the
uses when a Twitter
ember or wants to
n info."

Common issues with social networking

- Who are you really communicating with?
  - Has their account been compromised?
  - Has the provider of the tool/service been compromised?
- The content?
  - Has it been tampered with?
  - Does it have an abbreviated URL?
    - What is it really?
    - Has it been tampered with?

How to stay safe

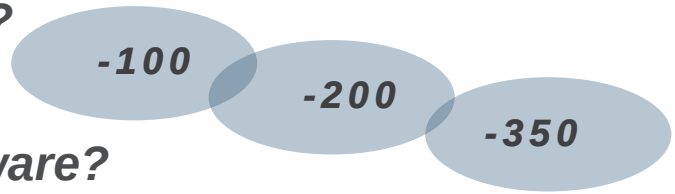
- Stopping users getting to compromised sites
  - Content filtering – Needs real time intelligence!

Digital Reputation – Risk Management

Length: ***How long has the domain or site existed?***

Width: ***How active is it?***

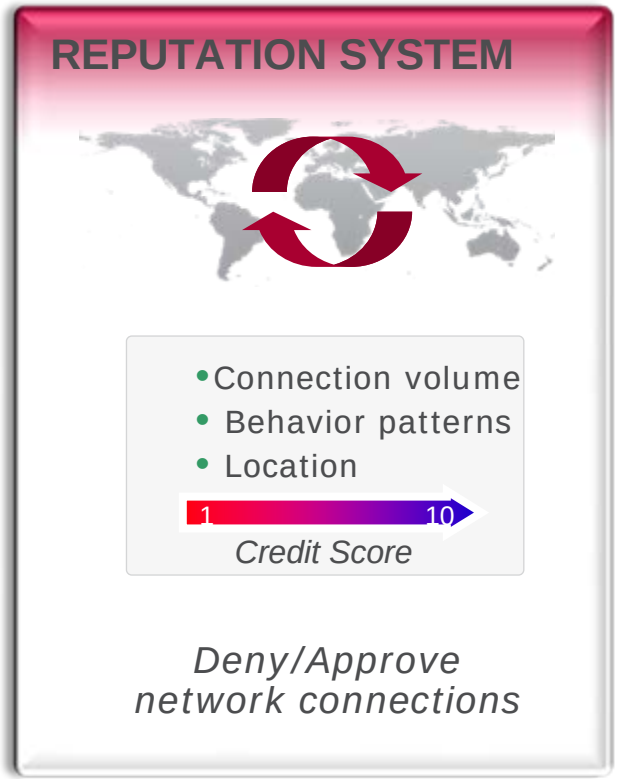
Height: ***Associated with spam or malware?***



Monitor Global Internet

Analysis using Global Threat Intelligence

Proactive Protection



Length: How long has the domain existed?
Height: How long has this behavior been recognized?

Reputation Score created using multiple dimensions. This score dynamically changes over time with improved or worsened behavior.

Reputation score used to decide whether the email is received or web page viewed.

- Stopping users getting to compromised sites
  - Content filtering – Needs real time intelligence!
- Ensuring users don't self infect
  - Anti-malware
  - Control what users can execute
    - User Access Control (Microsoft)
    - Whitelisting tools
      - Apple model - Digitally signed applications
      - 3rd party whitelisting tools
    - Behavioural controls (IPS, FW, etc)
      - Lock down OS
      - Control what can be installed, used, interaction with other resources)

Monitoring and controlling Social Networking usage

56% of employers admit to monitoring employees to see if accessing on-line social networking sites, amongst others things

38% block employees from accessing such websites

⅓ of employers have adopted policies limiting or prohibiting use of such sites during work time

6% have terminated employees for utilizing on-line social networking sites during work time

Source:http://www.hrtools.com/staffing/social_networking_survey_results_released_by_one_of_nations_largest_employment_law_firms.aspx
http://www.redorbit.com/news/technology/1558775/jackson_lewis_survey_finds_employers_screen_employees_use_0f_social/index.html
Research by : Jackson Lewis LLP Sept 2008

- Stopping users getting to compromised sites
  - Content filtering – Needs real time intelligence!
- Ensuring users don't sell infect
  - Anti-malware
  - Control what users can execute
    - User Access Control (Microsoft)
    - Whitelisting tools
      - Apple model - Digitally signed applications (Crackulous?)
      - 3rd party whitelisting tools
    - Behavioural controls (IPS, FW, etc)
      - Lock down OS
      - Control what can be installed, used, interaction with other resources)
- Data leakage
  - Education

Education?
Stop, think, act or NOT?

- Temporal lobe – flight or flight
  - Quick response
- Neocortex – analytical

UK alone, APACS reported £52.5m in online banking fraud losses

Source http://www

- Stopping users getting to compromised sites
  - Content filtering – Needs real time intelligence!
- Ensuring users don't sell infect
  - Anti-malware
  - Control what users can execute
    - User Access Control (Microsoft)
    - Whitelisting tools
      - Apple model - Digitally signed applications (Crackulous?)
      - 3rd party whitelisting tools
    - Behavioural controls (IPS, FW, etc)
      - Lock down OS
      - Control what can be installed, used, interaction with other resources)
- Data leakage
  - Education
  - Data Loss Prevention controls, DRM

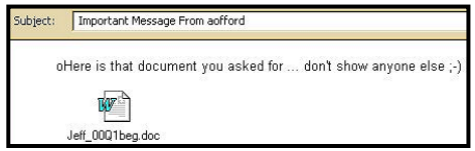
What can we expect in the future?

Misdirection tactics – adapted to today's tools

Common techniques

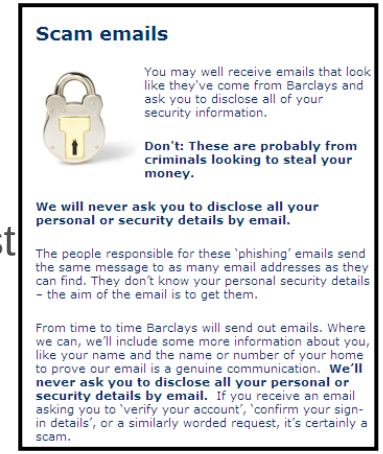
Then

- Position of Trust
  - AOL password stealing scams
  - Hoxes
  - Fake vendor updates/guidance
- Too good to be true
  - AOL4FREE
- Curiosity killed the cat
  - Don't tell anyone
  - Secret information
- A cry for love
  - Love letters



Now

- People you know and trust
  - Phishing scams
  - Social networking
- Too good to be true
  - Bogus Anti-virus
  - P2P sites boobitrapped
- Anything topical can kill the cat
  - Current affairs
  - Celebrities
  - Common words
- A cry for love
  - Online dating scams
  - Greetings card tricks



The future???

- Social engineering can be an easy route to customer
  - Only likely to increase as:
    - Security protection increases
    - Vulnerability/Patch management continues to improve

The future???

- Social engineering can be an easy route to customer
  - Only likely to increase as:
    - Security protection increases
    - Vulnerability/Patch management continues to improve
- We are making it easier for them to target us!

guardian.co.uk

News | Sport | Comment | Culture | Business | Money | Life & style

Sport › Football

Away days: Footballers' homes targeted by thieves

The robbery at Darren Fletcher's homes is the latest in a series targeting players who were known to be on duty for their clubs

Peter Walker
guardian.co.uk, Tuesday 24 February 2009 13.04 GMT
Article history

Darren Fletcher, the Manchester United and Scotland midfielder, has been the latest footballer to have his house burgled or robbed while he is away on playing duty.

More than a dozen footballers in the north-west of England have been targeted in the past two-and-a-half years,, among them nine playing for Liverpool. While some of the crimes have been linked — one man was jailed for burgling six Liverpool stars' homes — police believe others have been the work of copycat or opportunistic thieves.

The incident at Fletcher's home is the third in recent months in which attackers have threatened relatives at knifepoint.

The future???

- Social engineering can be an easy route to customer
  - Only likely to increase as:
    - Security protection increases
    - Vulnerability/Patch management continues to improve
- We are making it easier for them to target us!
- How much cybercrime will use malware vs social engineering to steal data?

- Q: Are you invest appropriate time/resources into stopping social engineering?

Greg_Day@McAfee.com

01000111011100100110010101100111010111110100010001100001011110010100000001001101011000110100000101100110011001010110010100101110011000110110111101101101