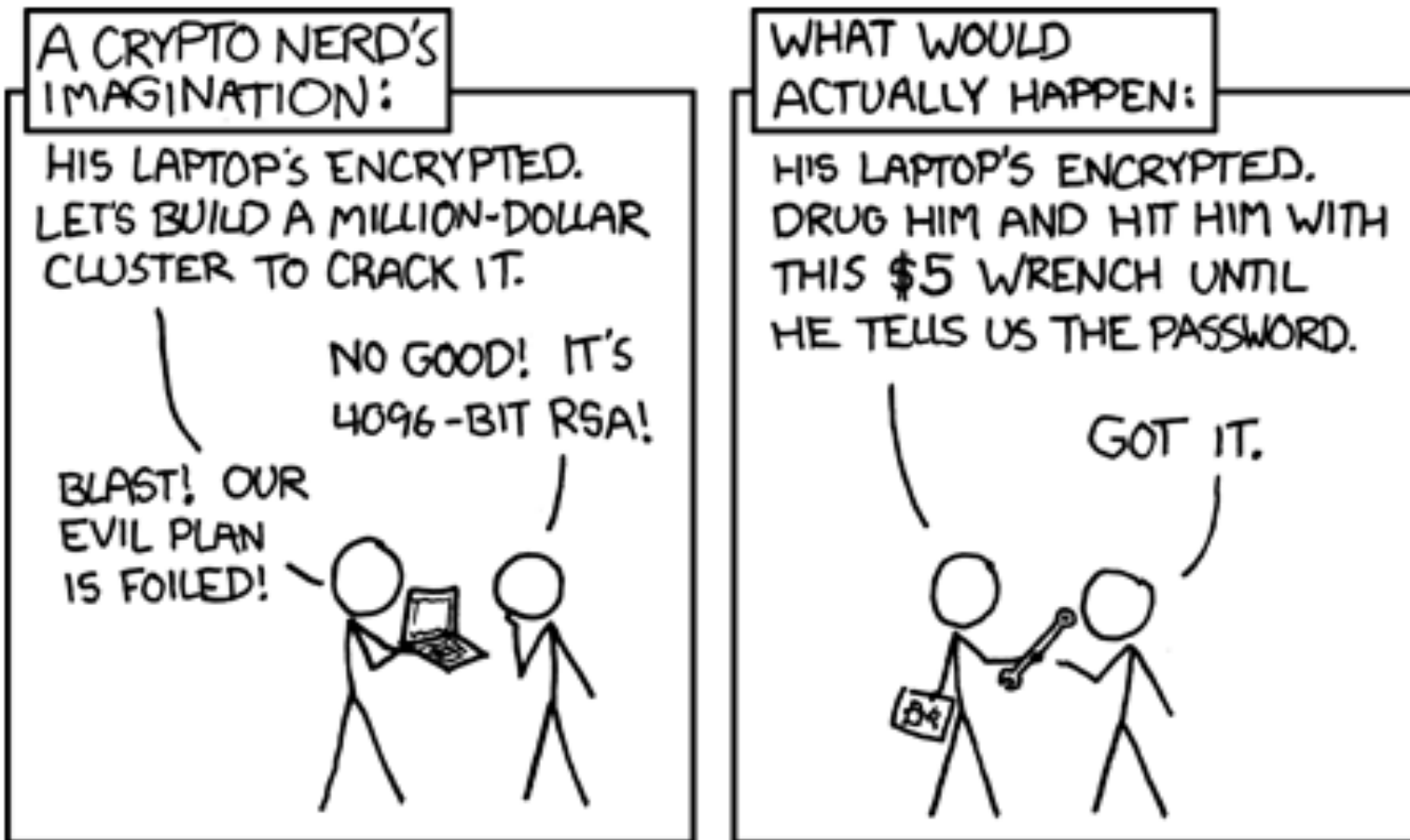


Intro Fun





Security & Trust

Trends on security and trust within the Internet – A focus
on Phishing trends and some solutions

The concept and details set out herein are preliminary and informative in nature only. Detailed analysis and validation of specific corporate proposals are ongoing. Implementation of any initiatives will be done in accordance with applicable contractual and legal obligations. Copyright © 2011 Edgemount Solutions, LLC. All rights reserved. All other names and data where referenced are trademarks or property of their respective owners.



Background

- In the past several months a series of highly sophisticated and targeted cyber attacks has revealed a shift in the threat arena and their persistence on networks (APT buzz)
- Attackers are moving beyond schemes to acquire financial data (such as credit cards and identity theft) and are pursuing high-value digital assets such as intellectual property, access to critical operations, and other proprietary data systems
- We are involved with businesses in attempt to review possible strategies and validation of business models that aim to offer mitigation against a portion of this space.



Social Engineering

- Most recent compromises that are reported use a technique called social engineering
- Defined - social engineering is using deception, manipulation, and influence to convince a human who has access to a computer system to do something, such as click on an attachment or a link in an email
- Social-engineering schemes historically use spoofed e-mails purporting to be from legitimate businesses and agencies to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as usernames and passwords.
- Recent attacks now bundle this method via spear phishing, which leads to a much more targeted attack; in order to access to a key person's workstation, data, etc.





Spear Phishing

- Phishing is a mechanism that employs both social engineering and malicious means to steal identity & financial account credentials
- Defined – Phishing is the act of tricking someone into surrendering private information over the Internet, follows the idea of actual fishing — you throw out bait with the hopes that while some ignore it, others will bite.
 - Traditional attacks mimic financial sites to collect credentials or online shopping sites to collect credit card data
 - Attacks most commonly come in the form of emails or messages that contain viral links.
- Recent trends show an increase of compromises that use techniques to allow an attacker access to a key person





Increased Effectiveness - Social Networking

- Social Networks make it easy.....one can go into Twitter, Facebook, LinkedIn, etc. to search for someone or use current events to lure recipients to react to a communication
- Online communities are powerful, trusted and perfect for cyber crime to leverage such relationships
 - Social networking attacks leverage a trusted link between friends, either to deliver malware or to phish for confidential and financial information.
 - Easier for attackers to spread malicious software through links, photos and applications because those users are typically more trusting





Increased Effectiveness - Social Networking

- At the end of 2010, nearly 85 percent of recorded phishing attempts used social networks as a lure, up from 8.3 percent at the start of the year
- Tiny URLs have also enabled better hiding of phishing domains from users. Phishing detection software generally looks for HTML-based content, hence some attacks are using Flash, JavaScript and MIME type content that autocorrects to HTML in browsers for success

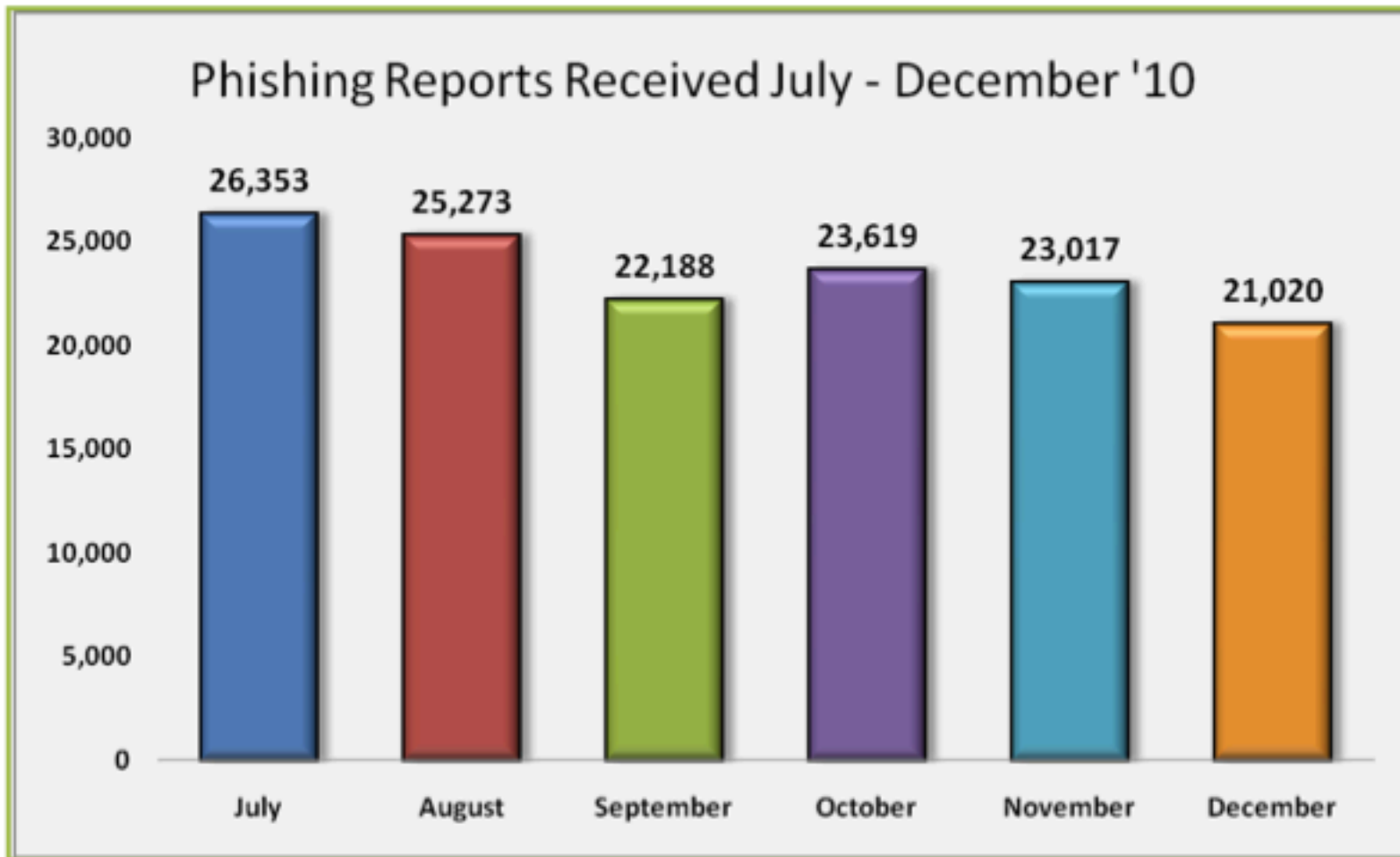


bitly



Phishing Trends – Reports 2H2010

- Phishing reports submitted to APWG during the second half 2010

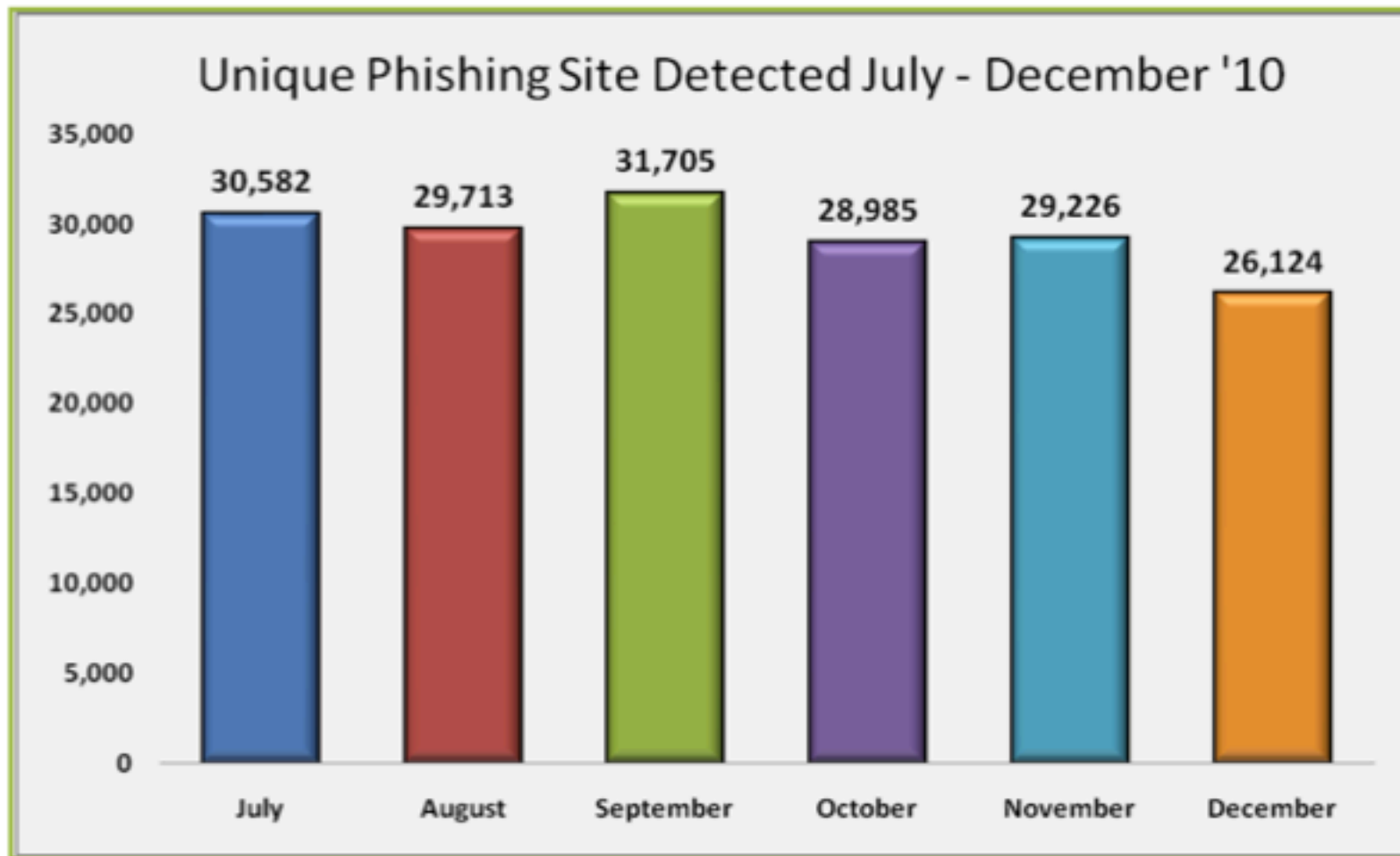


Statistics sourced from APWG Global Phishing Survey 2H2010 (April 2011). Data and examples contained herein are provided for informative use only.



Phishing Trends – Sites Detected 2H2010

- Sites reported to APWG reached the highest point in September 2010



Statistics sourced from APWG Global Phishing Survey 2H2010 (April 2011). Data and examples contained herein are provided for informative use only.



Trends -2H2010

- Phishing Trends per APWG (member report):

	July	Aug.	Sept.	Oct.	Nov.	Dec.
Number of unique phishing email reports received by APWG from consumers	26,353	25,273	22,188	23,619	23,017	21,020
Number of unique phishing web sites detected	30,582	29,713	31,705	28,985	29,226	26,124
Number of brands hijacked by phishing campaigns	274	301	335	317	305	279
Country hosting the most phishing websites	Sweden	Sweden	Sweden	USA	USA	USA
Contain some form of target name in URL	82.82%	95.13%	92.94%	79.93%	76.44%	75.86%
No hostname; just IP address	1.45%	0.84%	1.93%	3.89%	15.11%	3.05%
Percentage of sites not using port 80	0.12%	0.10%	0.23%	0.60%	0.43%	0.48%



Phishing Trends - Global

- Phishing trends saw a global increase (vs APWG member rpt)
 - Average site uptime – 73 hours (longest measurement)
 - Age of site ? (turnaround - currently reviewing)

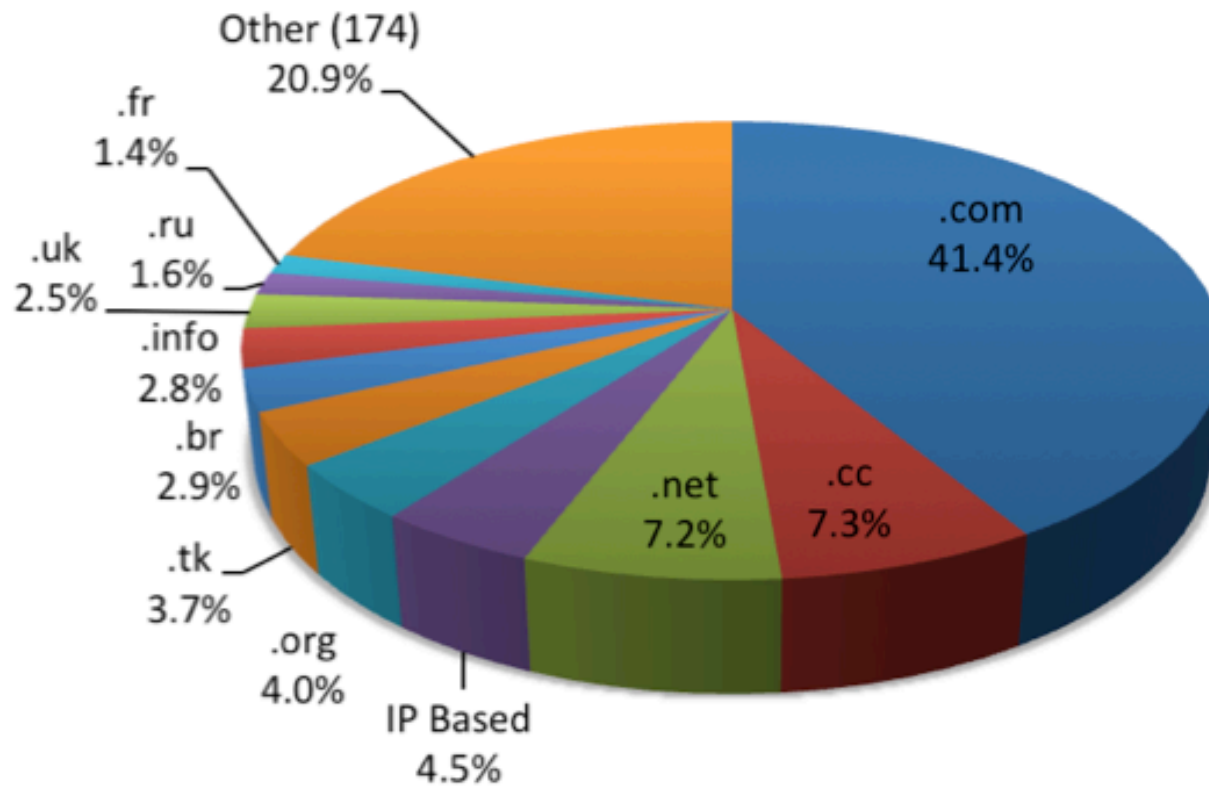
	2H2010	1H2010	2H2009	1H2009	2H2008
Phishing domain names	42,624	28,646	28,775	30,131	30,454
Attacks	67,677	48,244	126,697	55,698	56,959
TLDs used	183	177	173	171	170
IP-based phish (unique IPs)	2,318	2,018	2,031	3,563	2,809
Maliciously registered domains	11,769	4,755	6,372	4,382	5,591
IDN domains	10	10	12	13	10



Trends 2H-2010

- Phishing Attacks by TLD:

All Phishing Attacks, by TLD 2H2010

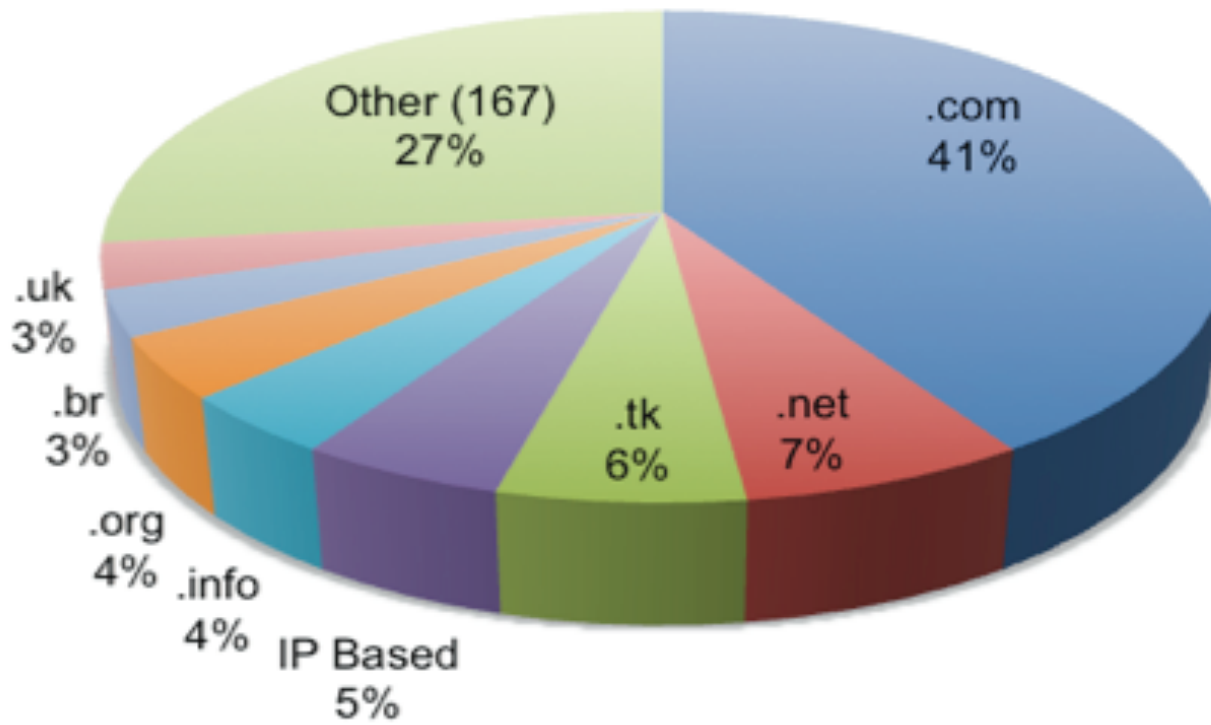




Trends Q2-2011

- Phishing Attacks by TLD:

PHISHING BY TLD - Q2 2011





AV Solutions – Impact or Lack Thereof

- Methodology generally ineffective against antivirus clients given lag in detection rates (cat & mouse)
- Malware Detection Rates by AV Vender (2010):

	Trend Micro	Sophos	McAfee	Kaspersky	F-Secure	Dr Web	AVG	Nod32	F-Prot	Virus Buster	Norman	eTrust-Vet	Symantec
Day 1	17%	20%	22%	22%	27%	7%	13%	37%	17%	10%	17%	16%	21%
Day 8	29%	36%	53%	87%	50%	29%	85%	86%	23%	30%	29%	21%	36%
Day 15	32%	75%	85%	91%	59%	33%	92%	88%	34%	46%	31%	27%	43%
Day 22	32%	81%	86%	92%	62%	33%	92%	88%	37%	74%	32%	29%	46%
Day 30	38%	85%	86%	92%	64%	33%	93%	89%	39%	74%	32%	30%	47%



Methods of the Attack

- Reconnaissance to build knowledge of organization/-target
- Social engineering and/or spear phishing to target end users
- Exploitation of vulnerabilities at end point
- Expand to peer relationships to roam the network
- Escalation of privileges / rights
- Additional spear phishing or decrypting
- Administrators' passwords
- Compromise of internal systems
- Exfiltration of data or other
- Cleanup





Examples of the Typical Attack

- Earthquake (Haiti / Chile)
- Japan Earthquake & Tsunami
- Chilean miners
- Poland President
- Gulf oil spill
- Michael Jackson



MICHAEL JACKSON TRIBUTE SET

MICHAEL JACKSON KEEP THE DREAM ALIVE

DON'T WAIT!
LIMITED 30-DAY RELEASE!

Moonwalk Print FREE Portrait

Michael – Moonwalk Print & FREE Professional Print

We have an incredible offer for you! You can order another phenomenal, limited edition, fully licensed Michael Jackson commemorative lithograph for the same incredible price of just \$10 and only \$6.99 shipping and handling.

This print depicts M.J. during his iconic performance of "Billie Jean" on the "Motown 25: Yesterday, Today, Forever" television special – just before he did his famous "moonwalk" for the first time on TV!

But that's not all! When you order the "Moonwalk" print, we'll also include yet another stunning Michael Jackson lithograph, his professional portrait in an amazing black and white print, for just separate \$6.99 shipping and handling.

So, how many sets of the special Michael Jackson "Moonwalk" lithograph along with the stunning professional portrait lithograph would you like today?

©2009 All Rights Reserved.



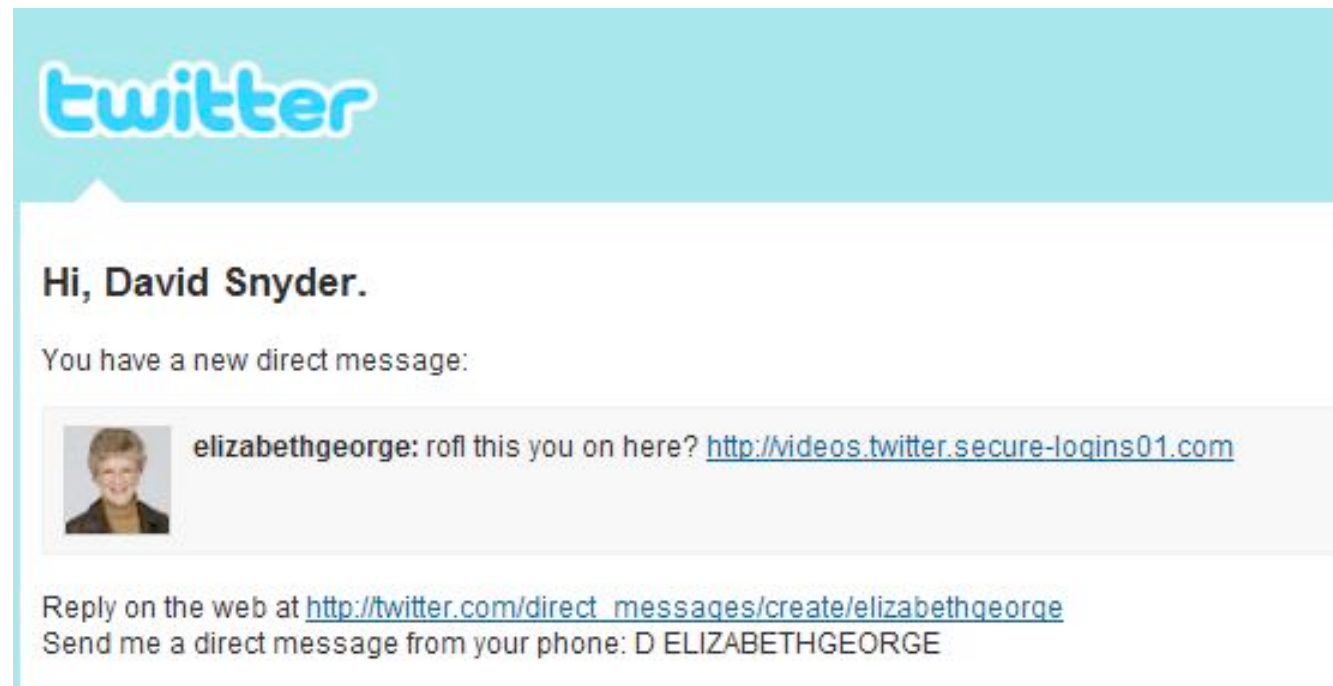


Examples of the Attack

- “Is this a video of you? <link>” sent from a trusted friend to a circle of friends quickly infects new systems to propagate to the next layer of friends



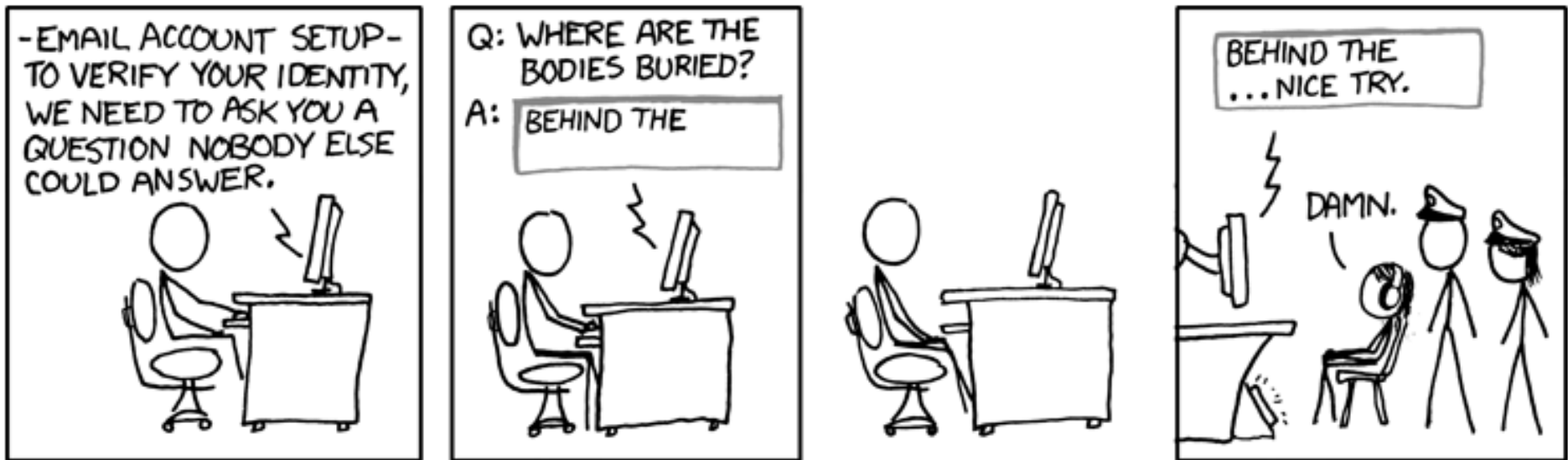
bitly





Another Possible Example

- Security Question – Password Update:





Recent Sophisticated Examples

- Most recent sophisticated compromises reportedly used spear phishing which allowed the attacker access to a key person's workstation:
- IMF: International Monetary Fund (IMF): 2011 attack gained access via spear phishing employee
- Google: Early 2010 – Attackers were able to install spyware on the resilient networks by manipulating key employees who had access to sensitive data to click on malicious links that exploited an Internet Explorer zero-day vulnerability. The attacks were timed for the holidays when IT administration is thinly staffed to cover operations.
- Q1 RSA SecurID data compromise occurred when an RSA employee clicked on a malware link in an apparent communication from a Human Resources department.





Questions Your Organization Should Ask

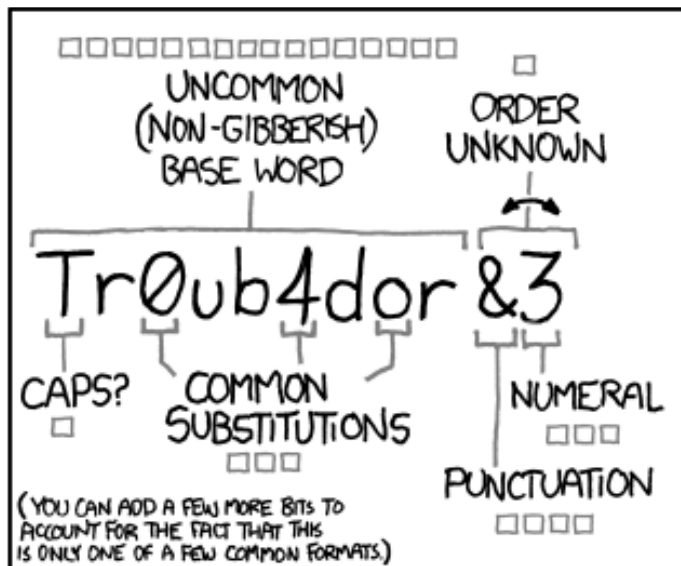
Q: How many of our users would fall prey to a spear-phishing attack?

Q: Would attackers be able to hijack admin accounts?

Recent examples raise questions about important web defense strategies such as protecting remote users and office-based workers through 24/7 security...



Do Current Efforts Make Sense?



~28 BITS OF ENTROPY

□□□□□□□□ □
□□□□□□□□ □□□
□□□□ □

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

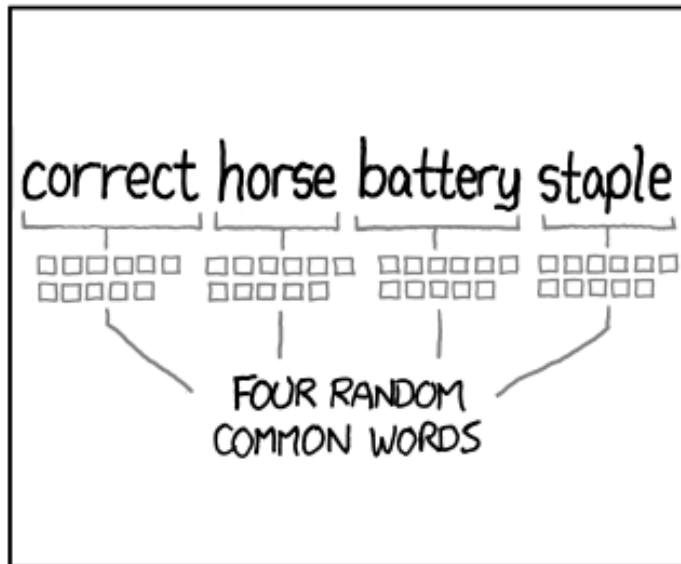
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOKEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

Stick-figure strip humor sourced and courtesy of <http://xkcd.com> and is provided for informative use only.



What Do We Do?

- Everything - There is no one solution
- Need to use a mix of user education and layered security solutions to defend the networks
- Employees should treat emails with suspicion and IT teams should leverage multiple resources (AV, IDS, User Restrictions)
- Some other ideas:
 - Products that send phishing emails to your employees safely and easily trains your employees - immediately - when they fall for an attack
 - Gathers actionable data to finely target future employee training and how to avoid the ever evolving threat on the Internet.
 - Complete formal spear phishing awareness training
 - Separate corporate and open systems – create an “air gap”
 - If data exfiltration is discovered, collect intelligence such as: What did they take, Where was the vector, How Long, Did they Leave, Where was it sent




Mitigation Examples

- User Training Examples:

The PhishGuru


Protect yourself from Phishing Scams

Clicking on links like the one in the "amazon.com" email you've just read puts you at risk for **identity theft** and **financial loss**. This email and tutorial were developed by **Carnegie Mellon University** to teach you how to **protect yourself** from these kind of **phishing scams**.



Simple ways to identify phishing scams

- Looks genuine but can be spoofed
- Looks genuine but can be spoofed
- Urgent messages
- Account status threat
- Links don't match with status bar when mouse is moved over



Simple definition of phishing

- Scammers send fake emails impersonate you into giving them your personal info
- Giving up your personal information is credit card number, or account pass financial loss.

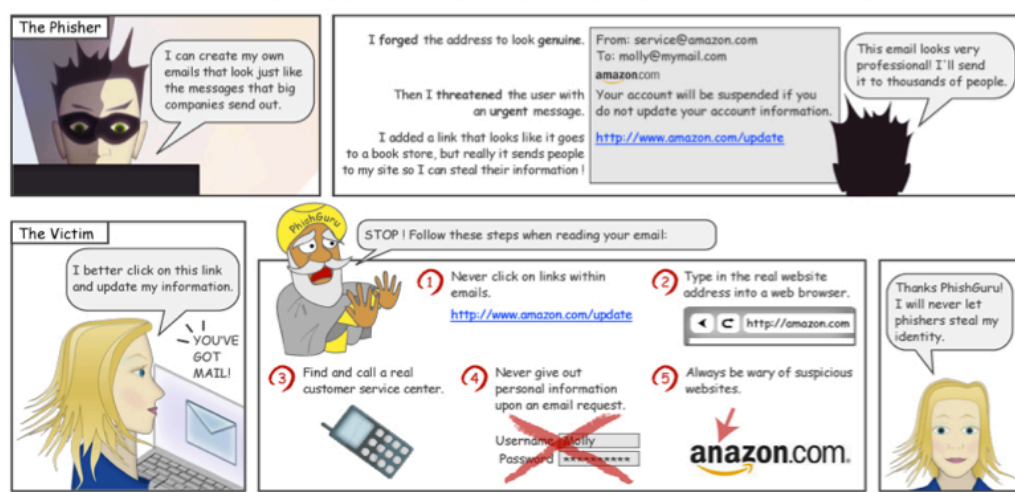
Simple ways to protect yourself

- Never click on links within emails or rep information.
- Always access a website by **typing in the real website address** into the web browser.
- Never trust phone numbers within emails. Look it up yourself and **call customer service** when email seems suspicious.
- Never give out personal information as companies will rarely ask for your personal information via emails.
- Be suspicious of websites that ask for too much personal information.

The PhishGuru

Protect yourself from Phishing Scams

Clicking on links like the one in the "amazon.com" email you've just read puts you at risk for **identity theft** and **financial loss**. This email and tutorial were developed by **Carnegie Mellon University** to teach you how to **protect yourself** from these kind of **phishing scams**.



The Phisher

I can create my own emails that look just like the messages that big companies send out.

I forged the address to look genuine.

Then I threatened the user with an urgent message.

I added a link that looks like it goes to a book store, but really it sends people to my site so I can steal their information!

From: service@amazon.com
To: molly@mymail.com
amazon.com
Your account will be suspended if you do not update your account information.
<http://www.amazon.com/update>


This email looks very professional! I'll send it to thousands of people.

The Victim

I better click on this link and update my information.

I - YOU'VE GOT MAIL!

STOP! Follow these steps when reading your email:

- Never click on links within emails.
<http://www.amazon.com/update>
- Type in the real website address into a web browser.
- Find and call a real customer service center.
- Never give out personal information upon an email request.
Username: molly
Password: *****
- Always be wary of suspicious websites.


Thanks PhishGuru! I will never let phishers steal my identity.



Thoughts

- The real issue isn't the type of mechanism being used to target victims, It's that users are simply not learning how to avoid being tricked on the Internet



Our Pending Solution – “Guidon”

- Understanding that when information is shared by a user the victim knows, attackers assume (generally correctly) that the attempt will be more successful
 - Example 1: You see a message from a friend or a link on your Facebook news feed. You click on it only to find..... common scams
 - Example 2: You continue to get messages from your father/friends
- Edgemount Solutions Pending Tool Development:
 - Leverage historical metadata analysis for trend
 - Global IP – Country location
 - Mail Client – Proxy service (known or unknown)
 - Time of message
 - Age of IP Domain
 - Trend based on historical dates
 - Various modes: Grandparent, Parent, Technical User, Kids





References & Various Resources

- APWG (www.antiphishing.org/index.html)
- MAAWG (www.maawg.org/)
- McAfee Security Trends & Reports (www.mcafee.com/us/mcafee-labs/threat-intelligence.aspx)
- Verizon / Verizon Business Security (securityblog.verizonbusiness.com)
- Microsoft Security Center (www.microsoft.com/security)
- Wombat Security Technologies (www.wombatsecurity.com/contact)
- Carnegie Mellon University (cups.cs.cmu.edu/anti)



McAfee





Other Fun

