Online Security

Lawrence Snyder
University of Washington, Seattle

Online Security's Importance

- Being connected electronically to the I'net and WWW is now essential and interesting, but not everyone out there is your Friend
- The hazards:
  - Spam, harassment, distractions
  - Harm to your system – loss of data & software
  - Theft of personal information, e.g. passwords
  - Identity theft
  - Frauds and scams

Passwords – First Line of Defense

- Many, many people use stupid passwords like:
  - 1234, asdf, password, abc, 123456
- A good password is appropriate for situation
  - 6-8 characters; {digits, upper & lower case, special}
  - Not in dictionary, not associated with you
- Strategy:
  - Pick a topic: fave movies, Australia, football, etc.
  - ALWAYS use the topic; it's the key to remembering
  - Pick phrase
  - Transform phrase into PW in 4-5 steps

Example of Password

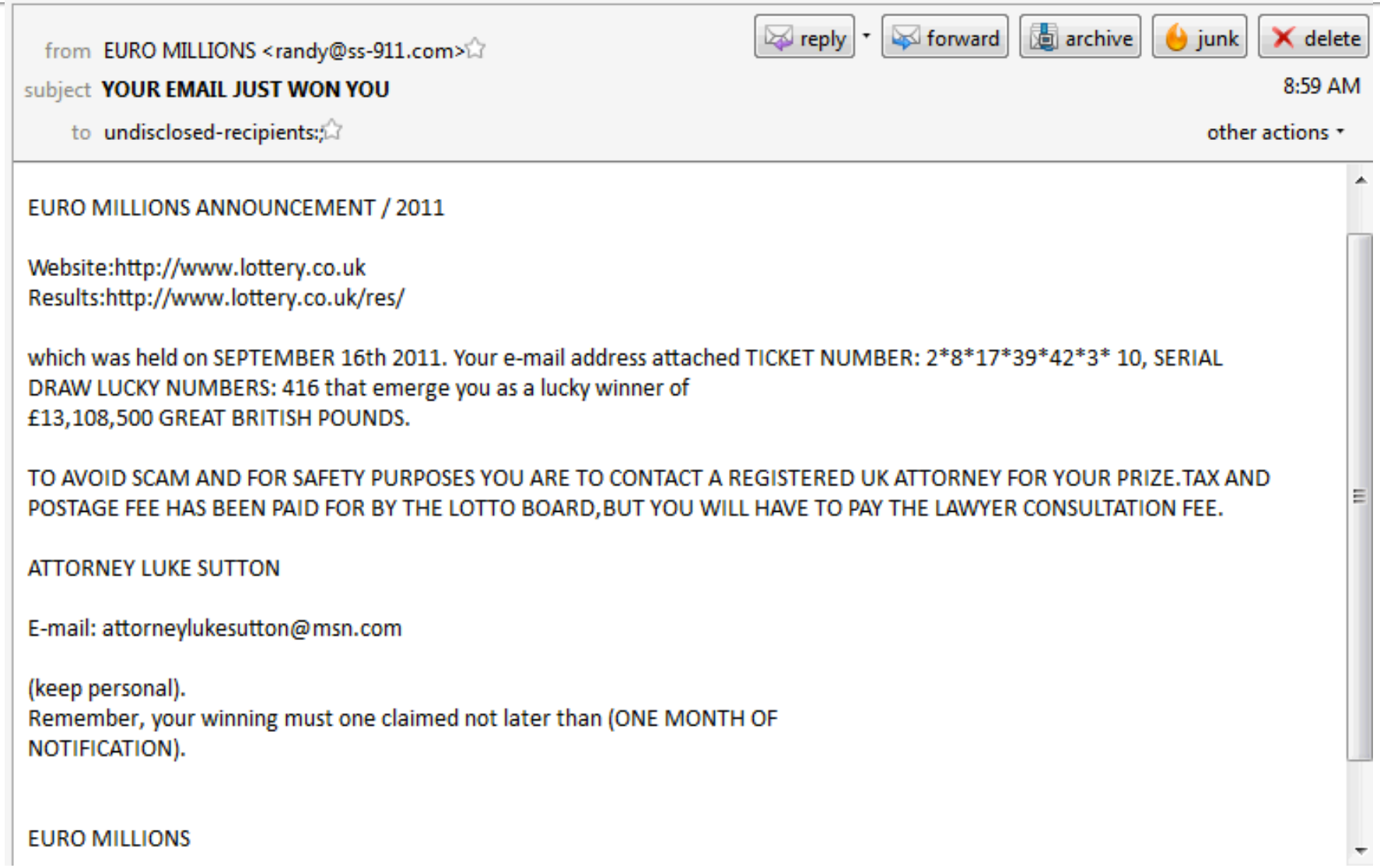
- Suppose your topic is "Movies"
- Begin with the title "The Matrix Trilogy"
  - Drop the "The", it's boring: MatrixTriogy
  - Change the "tri" letters to 3: Ma3x3logy
  - Change 3x3 to 9: Ma9logy
  - Change the capitalized letters: ma9Logy
  - Change "y" to "EE", o to 0: ma9L0gEE

This password is good for banking and other secure situations – you need weaker ones, too

Scams and Frauds: Nigerian Widow

- There are hundreds of these scams
- Technically they are called "advanced fee frauds" or "419 Scams" or "Nigerian Widow Scams" – they PREDATE the Internet!
- How it works
  - A person with a sad story needs your help; they have a lot of money they'll share as a "thank you"
  - You agree to help
  - Something goes wrong; they need a little money; you pay thinking it's a small amount compared to ultimate payoff; REPEAT

Scams and Frauds: Nigerian Widow



reply | forward | archive | junk | delete

from EURO MILLIONS <randy@ss-911.com>
subject **YOUR EMAIL JUST WON YOU**
8:59 AM
to undisclosed-recipients:;
other actions

EURO MILLIONS ANNOUNCEMENT / 2011

Website:http://www.lottery.co.uk
Results:http://www.lottery.co.uk/res/

which was held on SEPTEMBER 16th 2011. Your e-mail address attached TICKET NUMBER: 2*8*17*39*42*3* 10, SERIAL DRAW LUCKY NUMBERS: 416 that emerge you as a lucky winner of
£13,108,500 GREAT BRITISH POUNDS.

TO AVOID SCAM AND FOR SAFETY PURPOSES YOU ARE TO CONTACT A REGISTERED UK ATTORNEY FOR YOUR PRIZE.TAX AND POSTAGE FEE HAS BEEN PAID FOR BY THE LOTTO BOARD,BUT YOU WILL HAVE TO PAY THE LAWYER CONSULTATION FEE.

ATTORNEY LUKE SUTTON

E-mail: attorneylukesutton@msn.com

(keep personal).
Remember, your winning must one claimed not later than (ONE MONTH OF NOTIFICATION).

EURO MILLIONS

Review Structure of Net Address

- Notice this structure –

http://www.somename.com/foldera/folderai/file.html

Most important: Inspect this part (after the double slash and before the first single slash) carefully

Phishing … Social Engineering

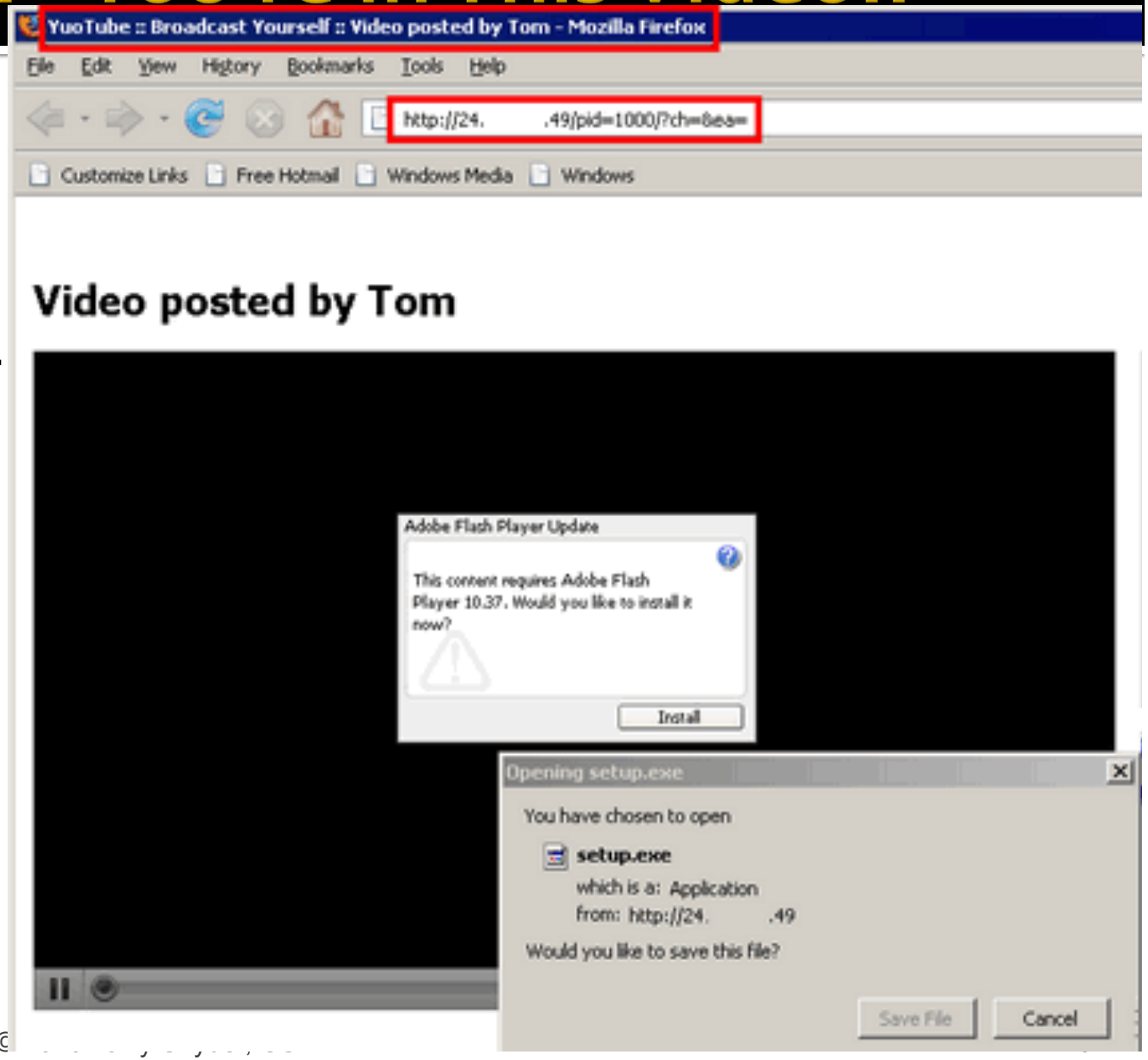
- "Phishing" is a term for tricking a user into giving personal information – easier than theft
- Have you seen mail like this …
  - "Your Email space is almost full – please fill out this form to get more space"
  - "Suspicious activity in your account – temporarily closed; contact us to resolve it"
  - "Our site has been attacked; accounts are closed; contact us to reopen your account"
- The site is fake; you give info; thieves have it!

Read The URL – It's Important Data

- How to collect FB accounts with password

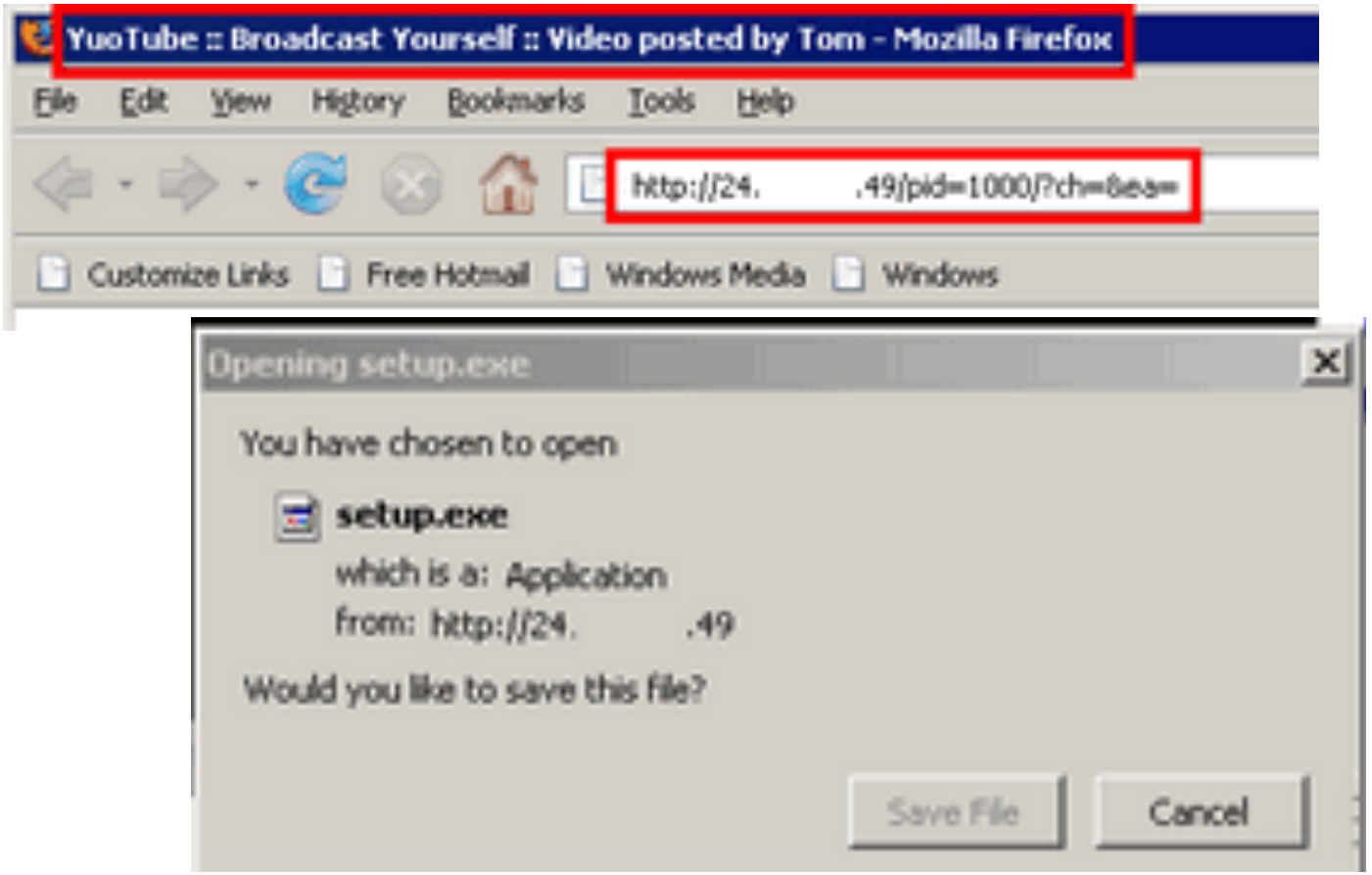
Koobface: "You're In This Video!!"

You click on the link. The fake site says your new version of Flash … don't do it! It's not Flash



Analyze The Data

- Before "taking the bait" notice the features of the site:



Installing Software

- Without a doubt, the riskiest thing you do on your computer (laptop, phone, whatever…) is installing software – but you NEED software!
- What to avoid: NEVER install software from an unexpected source, e.g. pop-up
- What to do [1]: Always visit the vendor's Web site or the App store to get legitimate SW
- What to do [2]: Set up your browser and your OS to get regular updates and install them b/c these typically have security updates

Five Vectors of Attack - 1

Email Attachments	
Mechanism	An infected file is attached to email
Behavior to Avoid	Clicking on the attachment to open it
Result	The malware (usually a worm) runs, sending copies of the email and attachment to the names in your address book
Protect Yourself	Don't automatically open attachments; find out (from the sender) why it was sent if you are unsure, and what it is for

- Email Attachments – source of viruses and worms – self-replicating software with "bad" stuff included that "rides along on SW" or "mails itself" to friends
- Worst extensions:
  .exe, .zip, .js, .vba …

If your OS hides file extensions, you MUST start displaying them

Five Vectors of Attack - 2

Spoofed Links	
Mechanism	A hyperlink in an email or blog post has been changed to point to a different site.
Behavior to Avoid	Clicking on the link to jump to it
Result	The bogus site could be a phishing site or a setup to install infected software
Protect Yourself	Avoid clicking on links in email from sources you do not know or links in on suspicious Web sites; it is wise always to copy/paste the URL in such cases

- This is "your account has been closed" case
- Be Alert – always look at WWW sites to assess if they are legitimate
- Reach important sites (credit card, etc.) by your bookmark, typing URL, googling for site …

Five Vectors of Attack - 3

Social Engineering	
Mechanism	You are presented with an unknown link to get something
Behavior to Avoid	Clicking on the link to visit it, and then installing software
Result	Your computer is seriously compromised, and often personal information such as passwords and account numbers is lost
Protect Yourself	Be skeptical when you are offered something for free, or told to install software from a site other than the vendor

- This is the "koobface" case – do not install software "given" to you … go get it yourself from the source (Adobe, MS, app store), so you know where it came from

Five Vectors of Attack - 4

P2P File Sharing

Mechanism	Files are transferred containing infected software or spyware
Behavior to Avoid	Installing software from unreliable sites
Result	Computer is seriously compromised, and often personal information such as passwords and account numbers is lost
Protect Yourself	Avoid P2P file sharing from unreliable sites; protect your computer with an up-to-date fire wall and virus protection software

- Peer-to-peer sites (file sharing) have special access to your computer –the easiest way to get a virus is to install infected P2P software
- Use only trusted sites – BitTorrent, Kazaa, Nutella, etc.

Five Vectors of Attack - 5

Bluetooth and MMS File Transfers	
Mechanism	Files are received by Bluetooth or MMS connections
Behavior to Avoid	Approving software installation
Result	Computer or phone is serious compromised
Protect Yourself	Install software only that you "go get" from the source

- Wireless connections have recently been used to share infected files – be alert at the coffee shop, airport, etc.
- Checking the files initiates a "install software" request – don't do it!

Encryption

- Encryption is the process of "scrambling" data so it is difficult (impossible?) to understand it
- We encrypt data to keep it private
- Every site that you use as https:// is encrypted
- Familiar example: Caesar cipher:

C: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
E: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- What would Julius be encrypted to?

Encryption

- Encryption is the process of "scrambling" data so it is difficult (impossible?) to understand it
- We encrypt data to keep it private
- Every site that you use as https:// is encrypted
- Familiar example: Caesar cipher:

C: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
E: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- What would Julius be encrypted to? Mxolxv

More Typically …

- The fixed shift of an alphabet is easy to break

Alternate:

- Sender uses a key, k, to "multiply" clear byte sequences (recall they're numbers) by key

-- Send encrypted result – looks like gibberish --

- Receiver "divides" by key to decrypt getting clear
- "Multiply" and "Divide" represent some invertible function; use mult & div in example

Example

- Let the clear be: "MEET @ 9" and key=13
- Break clear text into 2-letter sequences:
  - ME ET ♭@ ♭9
- Interpret text as numbers
  - 7769 6984 3264 3257
- Multiply by key:

7769×13=100997
6984×13=090792
3264×13=042432
3257×13=042341

- Send encrypted (6-digit) number
- Receiver does the reverse process …

An Alternate: Public Key Encrypt

- The problem with "private key" encryption: the two sides have to meet to agree on key
- Public Key fixes this: The receiver publishes (on Web site, say) a (very very special) key, K
- More importantly, the theory it uses means that *NO practical amount of computing can break the code*
- Here's what you do …

Public Key Process

- Sender breaks up the message into blocks as before
- Sender cubes each block – yup, raises to the 3rd power – and mods it by K, i.e. (<text>^{3})%K
- Transmit results
- Receiver raises each remainder to a high power determined by prime numbers & known only to him
- Receiver mods by *K*, too, which are

– surprisingly – the original blocks!

- The receiver assembles the message
- Thanks to Euler and Diffie & Hellman

This Is Amazing!!!