



Take a second to be secure.

The Security Minute

A communication of the Longwood University Information Security Office

March & April 2011

Read *The Security Minute* Online: www.longwood.edu/infosec

package delivery failure



Dear customer!
We failed to deliver postal sent on the 28th of April in time because the recipient's address is wrong. Please print out the invoice copy attached and collect the package at our department. UPS International.

We have recently seen an increase in the number of e-mails targeted at our users. These e-mails are made to look like they came from United Parcel Service (UPS), Federal Express (FedEx), or United States Postal Service (USPS) and they ask you to download an attachment or visit a website to obtain a "waybill", "airbill", "invoice", or "mailing label". These messages are a scam designed to have you download malware.

These service providers each posted an alert on their sites, advising users that they typically do not send unsolicited emails, let alone emails with attachments.

The image to the left is an example pulled from the UPS "Learn to Recognize Fraud" website

"UPS Tracking"

If the information is not correct or you have any questions, please call us at (888) 328-7450 and speak to a case manager. You can also use the "live chat" system located on our website.

Please call or email me if you have any questions, it would be my pleasure to assist you.

Arlene.
Senior Case Manager.

www.longwood.edu/infosec/alerts.htm

IN THIS ISSUE

SECURITY SPOTLIGHT:
COULD NOT BE DELIVERED

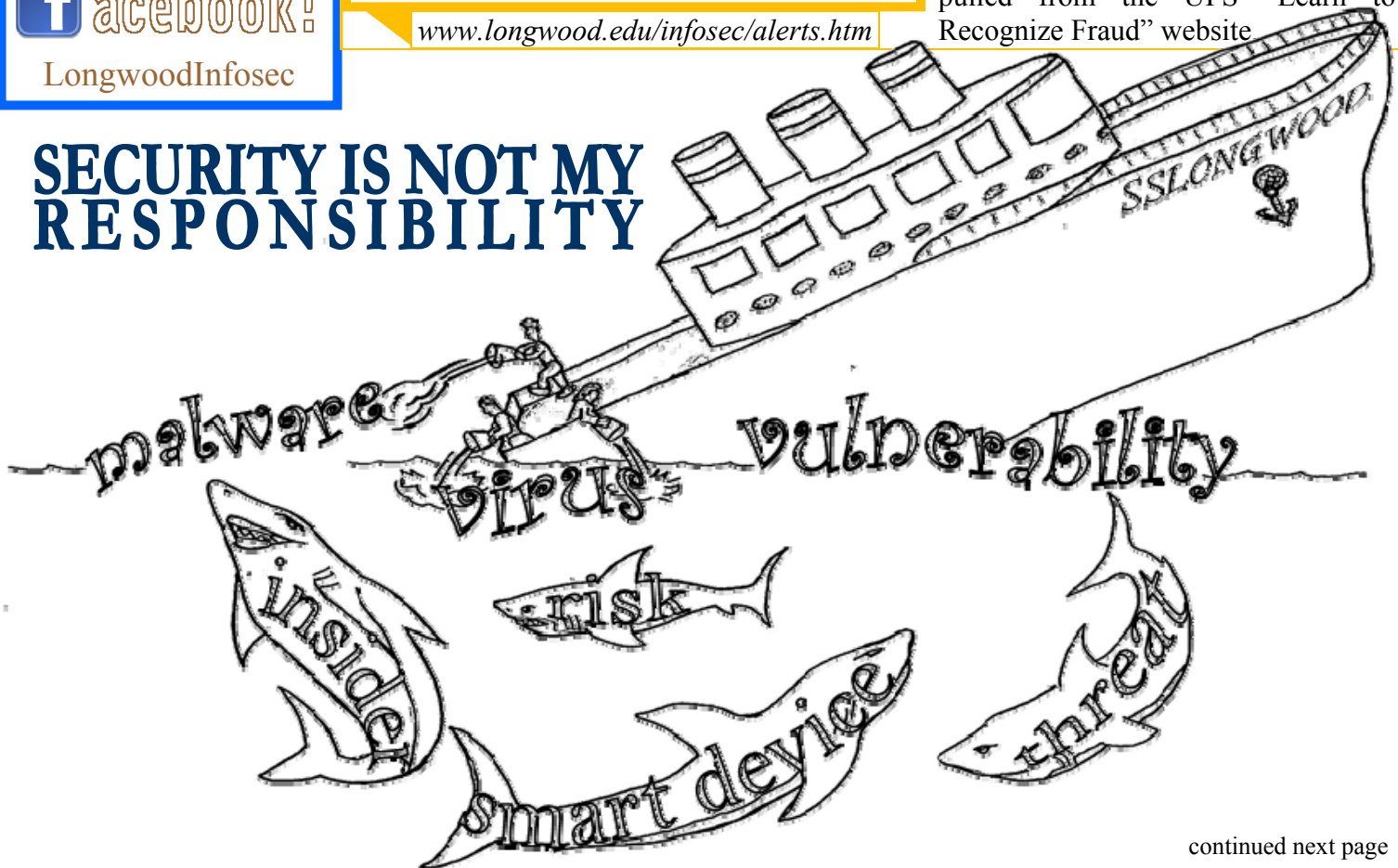
RUMOR HAS IT

HTTP vs. HTTPS

Security Spotlight:

We're on
 **acebook!**
LongwoodInfosec

SECURITY IS NOT MY RESPONSIBILITY



continued next page



The Security Minute is a monthly publication aimed at raising awareness of information security related issues and concerns. Please contact Jennifer Eckrote at 434-395-2034 or eckrotejl@longwood.edu.

HTTP vs HTTPS

Every time you type your username and password on a website that does not have <https://> you are essentially

username:	_____
doejk	_____
password	_____
Longwo0dl@ncerc	_____

broadcasting your login data for the world to see.

This article is paraphrased from an article, "HTTPS is more secure, so why isn't the Web using it?" (linked to www.facebook.com/longwoodinfosec) published by Scott Gilbertson, wired.com, March 2011.

The **s** implies the connection is more secure by making it much harder for someone to see what you are doing. But if <https://> is more secure, why doesn't the entire web use it?

<https://> is primarily used by sites that handle money—your bank's website or shopping carts that capture credit card data. Many sites that use <https://> only use it for the portions of their website that need it—like login pages and checkout pages.

Firesheep (2010) made it easy for anyone to capture data on insecure networks—coffeeshop's, restaurants and other public WiFi, which prompted many service providers to offer <https://> connections.

Sites such as Facebook, Twitter, Google, Wikipedia, etc all offer a <https://> connection. If you use the Mozilla browser Firefox, you can install the "HTTPS Everywhere" add-on to force <https://> connections to these sites, and many others, that offer <https://> but that do not use it by default.

There is no real reason the whole Web couldn't use <https://>. There are practical reasons why it isn't happening today, such as

- it's slower due to
 - the inability to cache web data.
 - the SSL key exchange.
- it costs more
- it doesn't work with virtual hosts (i.e. multiple sites using same physical server)
 - TLS extensions can make <https://> work with virtual hosts
- it doesn't make sense (i.e. users never log in to interact with website)

but eventually the practical problems will be resolved. In the Web of the future the main concern won't be how fast a site loads, but how well it safeguards you and protects your data once it does load.



The Security Minute is a monthly publication aimed at raising awareness of information security related issues and concerns. Please contact Jennifer Eckrote at eckrotejl@longwood.edu.

RUMOR HAS IT:

Revisiting the March 2008 edition of the Security Minute, my predecessor explained that "Technological controls offer a layer of security, but decisions we make as users are essential to protecting information and systems."

Security is everyone's responsibility. Avoiding an information security breach is everyone's responsibility. Handing data is what YOU do everyday, hence the responsibility being yours. YOU store data, YOU transmit data, and YOU dispose of data everyday.

Technology can help prevent an "OOPS", and the Information Security Office can help you help yourself. The image on the previous page shows, in the most non-technical way, that security is everyone's responsibility. By virtue of being a member of the Longwood community (people on the SSLONGWOOD),

protecting the University's data (the SSLONGWOOD itself) is YOUR responsibility (pick up a bucket and help already).

I know that it's easy to think that information security is the sole responsibility of the Information Security Office or some new piece of technology. However, our office and technology could miss a single wave or shark putting the entire campus at risk for a breach of the haul.

Policy Update:

At the March 25, 2011 meeting of the Board of Visitors four IITS policies revisions were approved, the CIO has also approved corresponding standards :

- Policy 6103: Encryption Policy
 - Minimum Encryption Standards
 - Encryption Key Management Standards
- Policy 6132: Incident Response
- Policy 6134: Data Classification
 - Data Handling Standards
 - Data Disposal Standards
- Policy 6135: Security Roles and Responsibilities

