

February 16, 2010

2010-02-16: Being safe in cyber world

Jenny Eriksen
Northeastern University

Recommended Citation

Eriksen, Jenny, "2010-02-16: Being safe in cyber world" (2010). *News@Northeastern*. Paper 516. <http://hdl.handle.net/2047/d20001759>

This work is available open access, hosted by Northeastern University.

Being safe in cyber world



Papageorge is the director of Northeastern's information assurance program. Photo by Lauren McFalls.

February 16, 2010

Cyber attacks, identity theft, credit card breaches, and computer viruses are some of the hazards associated with travel along the information superhighway. Information security is an urgent and ongoing concern for businesses and individuals alike. Themis Papageorge, director of Northeastern University's **information assurance** program, assesses the real risk associated with cyber threats, and offers advice on how to make our virtual journeys a little safer and more secure.

A recent survey of 600 information technology (IT) executives in 14 countries found that many believe that Internet security is a growing threat to society. Why is this

the case?

The number of cyber attacks has been increasing very quickly over the past 10 years due to the growing number of wireless and digital devices that people use in their daily lives. The impact of these attacks, from credit card theft to banking fraud, now affects the general public as well as large companies and government agencies. This accounts for annual losses totaling hundreds of millions dollars and threatens national security.

Since so many critical and highly sensitive industries, such as energy and banking, are using Web-based technologies, what infrastructure is necessary to keep proprietary information safe?

The infrastructure must combine cyber defense technology with societal awareness and education. People are behind these attacks. We need to educate and train IT professionals to use the best practices and technologies that are available to defend against cyber attacks. The general public also needs to be alert to potential attacks.

Since this is an international phenomenon, we need to collaborate and create a more comprehensive technical and legal framework to counter Internet security threats.

How extensive were the cyber attacks on Google in China?

Based on Google's public statements, the cyber attacks were deep and widespread. The attackers were able to penetrate Google's sophisticated defenses, resulting in the theft of Google's intellectual property and hundreds of thousands compromised e-mail accounts. In addition, Google identified at least 20 other companies that suffered Internet security breaches as a result of the same cyber attack.

If Google decides to leave China, how would that affect how information is shared to and from China over the Internet?

I think the impact will be significant, at least in the short term. From a business perspective it will take some time to replace the service that Google provides, quoted at \$600 million each year. From a technical point of view, Chinese and international companies that would step in to provide this service will have to put additional cyber defenses in place to thwart the next attack. In terms of U.S.-China relations, both governments have expressed very different views on this incident, which if not resolved, could restrict information sharing.

How will students enrolled in Northeastern's Information Assurance (IA) program be prepared to solve these problems?

The program trains students to become effective IA professionals and future chief security officers. Our students have technical or social science backgrounds that enable them to identify vulnerabilities and put technical countermeasures and policies in place to protect and defend organizations from Internet security threats. In addition, IA students graduate with both academic and business experience through experiential opportunities, better preparing them to meet real-world challenges.

Archives

The following news stories and features are available. For information about older content, please contact University Communications and Public Relations at (617) 373-5471.

2010

January
February
March
April
May
June
July
August
September
October
November
December

Share



Like

Sign Up to see what your friends like.

How can the general public help protect information shared over the World Wide Web and other interactive communications channels?

The general public can help protect their proprietary information by learning more about Internet security threats and using the available tools to make Internet access more secure.

If you have access to a virtual private network, which adds an extra layer of security, I would suggest using it. If you are accessing your bank account online, look for the URL to read "https," not "http," as the "https" designates that the information is secured by encryption. For e-mail communication, it is better not to open an e-mail or an attachment if you do not know the sender. Above all, educate yourself and be aware that "bad guys" are trying to breach Internet security measures every day, 24 hours a day, 365 days a year.

For more information, please contact Jenny Catherine Eriksen at 617-373-2802 or at j.eriksen@neu.edu.

[Northeastern Home](#) | [Find Faculty & Staff](#) | [Find A-Z](#) | [Search](#)

© 2010 Northeastern University · 360 Huntington Ave., Boston, Massachusetts 02115 · 617.373.2000 · TTY 617.373.3768