

TOM DAVIS, VIRGINIA,
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. MCHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LA TOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
MARSHA BLACKBURN, TENNESSEE
PATRICK J. TIBERI, OHIO
KATHERINE HARRIS, FLORIDA

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051
TTY (202) 225-6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER,
MARYLAND
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE

BERNARD SANDERS, VERMONT,
INDEPENDENT

"Protecting Our Nation's Cyber Space: Educational Awareness For the Cyber Citizen."

**Wednesday, April 21, 2004
2:00 p.m.**

Room 2154 Rayburn House Office Building

Opening Statement of Chairman Adam Putman (R-FI)

I want to welcome you all today to this hearing on "Protecting Our Nation's Cyber Space: Educational Awareness for the Cyber Citizen." In the past few years, the growth in access and use of the Internet, the increase in high-speed connections that are always on, and the rapid development and deployment of new computing devices has resulted in an expanding global computing network. Although these advances have improved our quality of life, this global network is susceptible to viruses and worms that can circle the world in just minutes...not to mention the potential of more malicious cyber attacks. While businesses, educational institutions, and home users enjoy the benefits of using the Internet, they are not often adequately informed about the potential dangers that their computer systems face if left vulnerable and unprotected. The good news is there are solutions and remedies to help mitigate the threats; the bad news is awareness of these solutions and the practice of safe Internet use is not far reaching. Attacks are evolving at a greater speed than preparation. This hearing will provide an opportunity for us to learn about the efforts of the Federal government, trade associations, corporations, and non-profits to raise awareness about the importance of cyber security. Today I call on all stakeholders to take immediate action...all of us have a role and a responsibility...to implement basic cyber security hygiene in order to reduce the potential vulnerabilities that could contribute to a successful cyber attack.

As use of the Internet all over the world grows, so do the presence and ambitions of people with criminal and malicious intent. Hackers attempt to take over people's computers to create ways to send spam, steal information and launch attacks undetected.

Criminals try to trick unsuspecting cyber citizens to reveal personal information by impersonating respectable web sites, a crime known as “phishing.” Consumers on the Internet may be tricked into downloading spyware. These programs may be harmless, yet extremely annoying, such as delivering a continuous stream of pop-up ads. Or they may be malicious, extracting information such as passwords and personal information for criminal purposes.

There are existing and emerging protections against these threats. Cyber citizens can arm themselves with virus protection software to help stop any potential impact of worms and viruses. Use of firewalls can help prevent some forms of spyware. Of course, after the rapid spread and dramatic impact of worms and viruses this past year, I think we all know the importance of keeping our systems patched and up to date. Security notices are everywhere reminding us not to open e-mail from people we don’t know, and not to download programs from unknown sources.

However, many Internet users, consumers, non-profits, educational institutions and businesses, do not employ these well-known protections. They are either unaware of the risks, or unaware of the solutions, or both.

User awareness is only part of the problem though. Many of the security problems that users face are rooted in products that were designed to deliver functionality, often without adequate regard to security. The manufacturers of both software and hardware products must accept responsibility in this area, and respond to the growing demands of the consuming public for improved quality and security. This Subcommittee has already held hearings on the proliferation of worms and viruses and on the issue of software assurance. And I will continue to pursue those issues. However, I am heartened by what I see as signs that the manufacturers are stepping up to the plate. I see an increased attention to security that seems to go beyond merely lip service. Manufacturers of all levels of notoriety are publicly confirming their commitment to providing consumers with products that are less “buggy” and more secure.

In an effort to dramatically improve information security throughout corporate America, I convened a group of 25 leaders from business organizations, as well as representatives from academic and institutional communities, to form the Corporate Information Security Working Group. The intent was to produce a set of recommendations that could form the basis of an action plan for improving cyber security for businesses and enterprises of all sizes and sectors. The group divided into subgroups, one of which was the Awareness, Education, and Training Subgroup. This subgroup’s mission was to identify, partner with and build on the good work of organizations that have or are developing campaigns that raise awareness on the importance of cyber security. Let me pause and acknowledge the tremendous work that Commissioner Swindle and the FTC have been pursuing for some time now. It is my view that our collective efforts CAN make a difference. The Awareness, Education, and Training Subgroup reported recommendations for three categories of users – small businesses, large enterprises, and home users.

For small businesses, the group suggested creating and distributing a Small Business Guidebook for Cyber Security that explains cyber security risks in terms that are readily understood and that motivates small business owners to take action.

For large enterprises, the Awareness, Education, and Training Subgroup suggested enhancing distribution of existing documents for large enterprise managers. Many organizations – including the Institute for Internal Auditors, the Internet Security Alliance, and the Business Software Alliance – have done good work in this regard. The group believes these documents deserve greater distribution, and will work with organizations representing large corporations to find the proper channels for broader dissemination. Furthermore for large enterprises, the group suggested creating a guide to information security for C-level executives, such as CEOs, CFOs, and COOs. A user-friendly guide for C-level executives is necessary to raise the profile of the information security issue in terms senior executives can understand. To that end, the group is currently working with representatives of large business organizations to see how it might collaborate on and distribute such a guide.

Finally, the group suggested targeted efforts aimed at the mass market would help to educate home users. The group is seeking to build upon existing relationships and to forge new partnerships between organizations, corporations, and the government that will help educate the home user base on cyber security.

One of the other Subgroups worked diligently on developing a set of best practices and guiding principles in information security that could apply from the most unsophisticated home user to the most sophisticated enterprise. Those efforts have produced incredible results, and provide a foundation for the Awareness, Education, and Training Subgroup to build upon.

In addition to my Corporate Information Security Working Group, there are several other organizations, including both public and private entities that are working to improve awareness and provide education to cyber citizens. This includes a broad base of constituent groups, including the education community. Today we will hear about awareness and education efforts in the K through 12 community, as well as in institutions of higher education. In addition to these awareness and education efforts, I am pleased to announce at this hearing two partnerships that the Department of Homeland Security is undertaking to train information security and assurance professionals through our Nation's colleges and universities. The Department will be partnering with NSA to enhance the Centers of Academic Excellence in Information Assurance Education Program to increase the number of information security professionals entering the work force. The Department will also be partnering with the National Science Foundation on its Scholarship for Service Program, which provides two-year scholarships for training information assurance specialists who in turn make a commitment to work for a Federal civilian agency for two years. I am looking forward to hearing more about these various initiatives in the testimony today.

I will note that I do have a concern. I worry that if we bombard our cyber citizens with too many messages from too many sources, they may become confused and take no action at all. If we are to begin a national, intensive campaign to educate individuals, and small and medium businesses on cyber security, I think we need to have a collaborative strategy that facilitates the delivery of a clear and common message about how folks can protect against the threat of a cyber attack. I look forward to hearing from today's witnesses that my concern is being addressed in a proactive and collaborative manner.

We must maintain the advantages that multiple channels give us for outreach and we must continue to recognize that one size does not fit all and that the required level of cyber security hygiene will vary depending on the profile of the user. Some basic steps are invariably common to most users and today we will identify steps being taken to convey that information. The more voices repeating the message, the more people are likely to hear it and pay attention. It would be difficult in my estimation and based on what I have learned to overstate the importance and timeliness of such an effort.

I look forward to the testimony from today's witnesses and I thank you for your contribution to the security of our Nation.