Three approaches to awareness: unified messaging, local responses, and National Cybersecurity Awareness Month

Michael Kaiser
Executive Director
National Cyber Security Alliance
michael@staysafeonline.org
About NCSA

Mission:

NCSA’s mission is to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals’ use, the networks they connect to, and our shared digital assets.

Vision

In a climate of persistent threats, securing cyber space is a responsibility we all share.

Securing the Internet and our shared global digital assets—cybersecurity—is critical if we are to achieve the potential of an empowered digital society capable of leveraging robust and widely available:

- content
- community
- communication
- commerce
- connectivity

NCSA builds strong public/private partnerships to create and implement broad reaching education and awareness efforts to empower users at home, work and school with the information they need to keep themselves, their organizations, their systems, and their sensitive information safe and secure online and encourage a culture of cybersecurity.
APWG/NCSA Online
Consumer Safety & Security Message Convention
The Project

• Unify Industry, Government, Non-Profit & Academia around cybersecurity awareness

• Motivate Americans to take action

• Create a culture of where cybersecurity is “second nature”
Why do it?

- Harmonize the message
- Cut through the cluttered marketplace of information and tips
- Raise safety and security messaging to = other social messaging
- Change behavior
- Address as a cultural issue
- It's not just about the message it's about getting it out
The Strategy

• Collaborate & Cooperate: a strong public-private partnership

• An attempt to rationalize and mature messaging

• Research: What message will motivate action?

• Create: a short, pithy tagline that resonates with the public & provide the supporting message platform
The Research

- Two focus group
  - Stakeholder
  - Consumer

- Nationwide survey
  - N=1,007
  - general public (18+)
  - online survey
Consumers are aware of what they need to do to be more secure online. Collectively, our messages about passwords, security software, firewalls, updates, etc. are known.

50% reported inaction due to either lack of knowledge or a belief that they are already doing enough.
Top Online Concern: Identity Theft

54% of Americans are extremely concerned about loss of personal or financial information

- 53% as concerned as losing their job
- 51% concerned about not being able to provide healthcare for their family (51%).
Personal Responsibility

• 96% feel a personal responsibility

• 93% said their online actions protect friends and family AND the greater community

• 61% feel that online safety & security is under their control
90% expressed a strong interest in learning more

Consumers are concerned about their own security and safety and are ready to learn. While they know there are things they need to do, they don’t have the information they need (for a variety of reasons) – and they want to be educated.
Our Opportunity

• The general public is ready for the type of broad scale, national campaign that will raise awareness AND educate about how to be safer and more secure online.

• “Safer For Me – More Secure For All” is the concept we are focusing on.
Negative and/or fear-based messages are counterproductive. Consumers want positive, action-oriented information about how to stay safe and secure online, although they can be motivated by facts about risk and prevalence.
Who is doing it?

• APWG and NCSA have led the effort

• Participants to date include:
  • Walmart, Costco, Facebook, Microsoft, McAfee, Intuit, SAIC, Lockheed Martin, ESET, AVG, Intel, TrendMicro, Google, Yahoo!, AT&T, Verizon, EMC, VeriSign ICSA, Visa, Symantec, Fox Interactive (MySpace), DHS, FTC, IRS, Social Security Administration, Department of Justice, White House (NSS staff).
  • Eventually many more!
To Solve A Global Problem

Build A Local Response
The Idea

Make cybersecurity like other social issues:

A priority at the community level.
Why Now?

• We are in the digital age
• Networks are everywhere
• We are not secure unless every network everywhere is secure
• Should there be a cyber attack, incident, or widespread outage, citizens will look to local leaders
• Our digital assets are everywhere
A Holistic Approach

- Engage Leadership
- Empower the Community
- Identify Existing Programs & Bring to Scale
- Fill the Gaps
- Launch a Comprehensive Community Campaign
- Establish Metrics to Measure Success
Stakeholders

Government

Community

Law Enforcement

Non-Profit

Education

Industry
The Internet is a Shared Resource

Securing it is Our Shared Responsibility

By activating all stakeholders we can accomplish more.
• Yours
• Mine
• Law enforcement
• Owners
• Everybody???
Industry
Law Enforcement
Media

An Opportunity to Educate
San Diego

Securing Our eCITY

Model Cyber City Project

www.securingleourecity.org
Vision

Create safe digital neighborhood that is both resistant to cyber-threats and resilient to man-made or natural disasters, where our citizens, businesses, organizations and government can effectively and securely navigate, collaborate and compete in today’s fast-changing technological environment. The secure cyber city model we establish in San Diego will empower our citizens and serve as a beacon for cities across North America and the world.
Enable every San Diegan to live, work and play safely in the cyber world.
Since December 2009

180 Stakeholders

• Industry
• Education
• Military
• Critical Infrastructure
• Local Business & Industry
• Law Enforcement
• Non-profit
• Community
• Local, State & Federal Government

• Mayor, City of San Diego
• California Chief Information Security Officer
• U.S. Attorney General
• 2 U.S. Congressmen
• Federal Bureau of Investigation
• San Diego County Sheriff
• San Diego County
• San Diego Police Department
• NAVY/SPAWAR
• San Diego Police Foundation
• San Diego Regional Chamber of Commerce
• San Diego Better Business Bureau
• Sony Corporation
• Cubic Corporation
• SEMPRA
• SAIC
• Booz Allen Hamilton
• The Security Network
• Manpower
• Step-Up San Diego and UCSD Extension
• San Diego State University
• San Diego Business Journal
Working Groups

- Law Enforcement
- Critical Infrastructure
- Education
- Awareness
- Cluster (economic development around cybersecurity)
- Metrics
- Public Private Partnership
- Policy (local, state, federal)
Washtenaw County Internet Safety Task Force

Mission/Vision Statement (Draft)

• Mission Statement: The Washtenaw County Internet Safety Task Force empowers community members through awareness and education to use the Internet and its related technology safely and securely.

Vision Statement:

• To create a digitally safe community.
The Task Force Approach

• Led by an elected official

• 45 members including representatives from: law enforcement, higher education, local media, children's services, school district, and chamber of commerce.

• Steering committee and larger group meet once each month
Objectives (abridged)

- Check with the IT departments at all agencies (and third party vendors) to be sure they have the resources needed to keep municipal networks secure and that all systems have current security software.

- When citizens report cybercrimes local police don’t have jurisdiction over, encourage them to report them to the FBI’s Internet Crime Complaint Center (www.ic3.gov).

- Review and update network and computer acceptable use policies for schools, departments, and townships.

- Encourage local technology companies to send volunteers to schools.

- Work with the local the school board, department of education, and parents to ensure that school curriculum is comprehensive and addresses cyber security, cyber safety, and cyber ethics.

- Initial efforts for this year focus on child safety, only as a gateway to larger cybersecurity issues.
And lets not forget....
What are you doing to educate...

• your students
• faculty
• staff
• community
michael@staysafeonline.org