

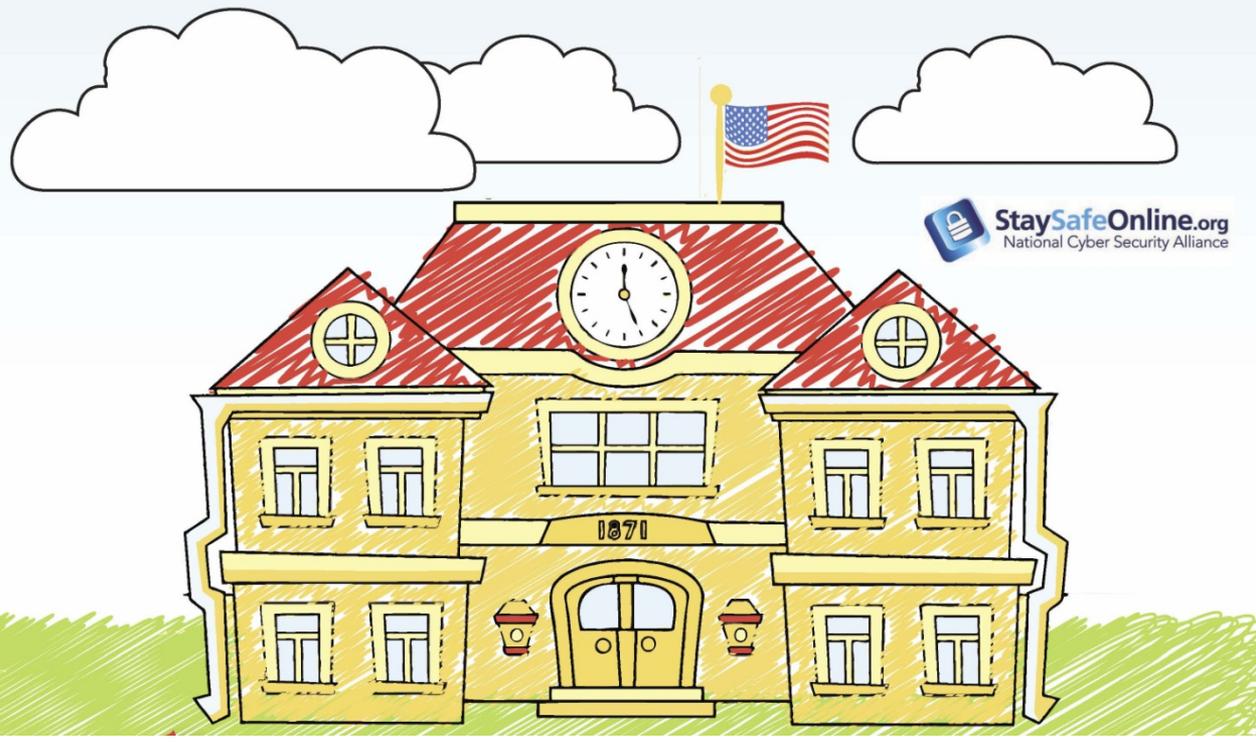
Zogby Analytics conducts a wide variety of surveys internationally and nationally in industries, including banking, IT, medical devices, government agencies, colleges and universities, non-profits, automotive, insurance and NGOs.

Based on 4 decades of polling and research experience, our advanced data collection and analysis deliver the data our clients require to make strategic decisions.

A new e-book by John Zogby and Joan Snyder
***The First Globals: Understanding, Managing,
and Unleashing Our Millennial Generation.***

First Globals - Americans born between 1979 and 1994 that are truly more globally aware and sensitive, how they want to make their workplace and planet a better place, and how we begin to understand them and position them better to play out their destiny.

STATE OF U.S. CYBER EDUCATION



TIME KIDS SPEND ONLINE

94% of TEENS
ages **12-17**
GO ONLINE...



58% of TEENS
have their own
ONLINE
PROFILE...

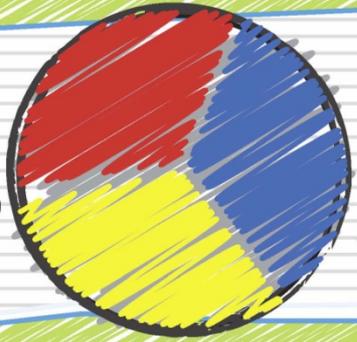


75% OF 12-17
YEAR OLDS
have their own
mobile phone



8-18 YEAR OLDS devote an
average of **7 HOURS AND**
38 MINUTES DAILY to
using electronic devices

- Kids Lead Digital Lives
- 33% ONLINE**
 - 33% OFFLINE** (awake)
 - 33% ASLEEP**



if a child **sleeps**
8 HOURS a night,
that means
ONE HALF of the
time he or she is awake
is spent online



**National Cyber Security Alliance,
McAfee and CyberSmart! Education
Team Up to Bring Cyber Security Learning
Resources to K-12 Classrooms after Zogby
survey shows teachers don't have the
resources needed**



"A recent study conducted by NCSA on the state of education in online safety, security, and ethics in K-12 schools found that only 24 percent of teacher's feel well prepared to teach issues related to cybersecurity, with many citing a lack of teaching resources," **said Michael Kaiser , executive director of the NCSA.** "We hope that these resources further empower teachers and students with the information they need to keep themselves and their information safe and secure online not only this October but every day of the year."




SCHOOLS NOT PREPARING KIDS FOR DIGITAL AGE

✓ 81% OF SCHOOL ADMINISTRATORS BELIEVE THEIR DISTRICTS DO AN ADEQUATE JOB PREPARING STUDENTS FOR CYBERSECURITY, CYBERSAFETY AND CYBERETHICS.

YET, THIS CONFIDENCE DOESN'T PLAY OUT IN THE CLASSROOM.

FEW TEACHERS ARE EDUCATING KIDS ON BASIC CYBER SKILLS

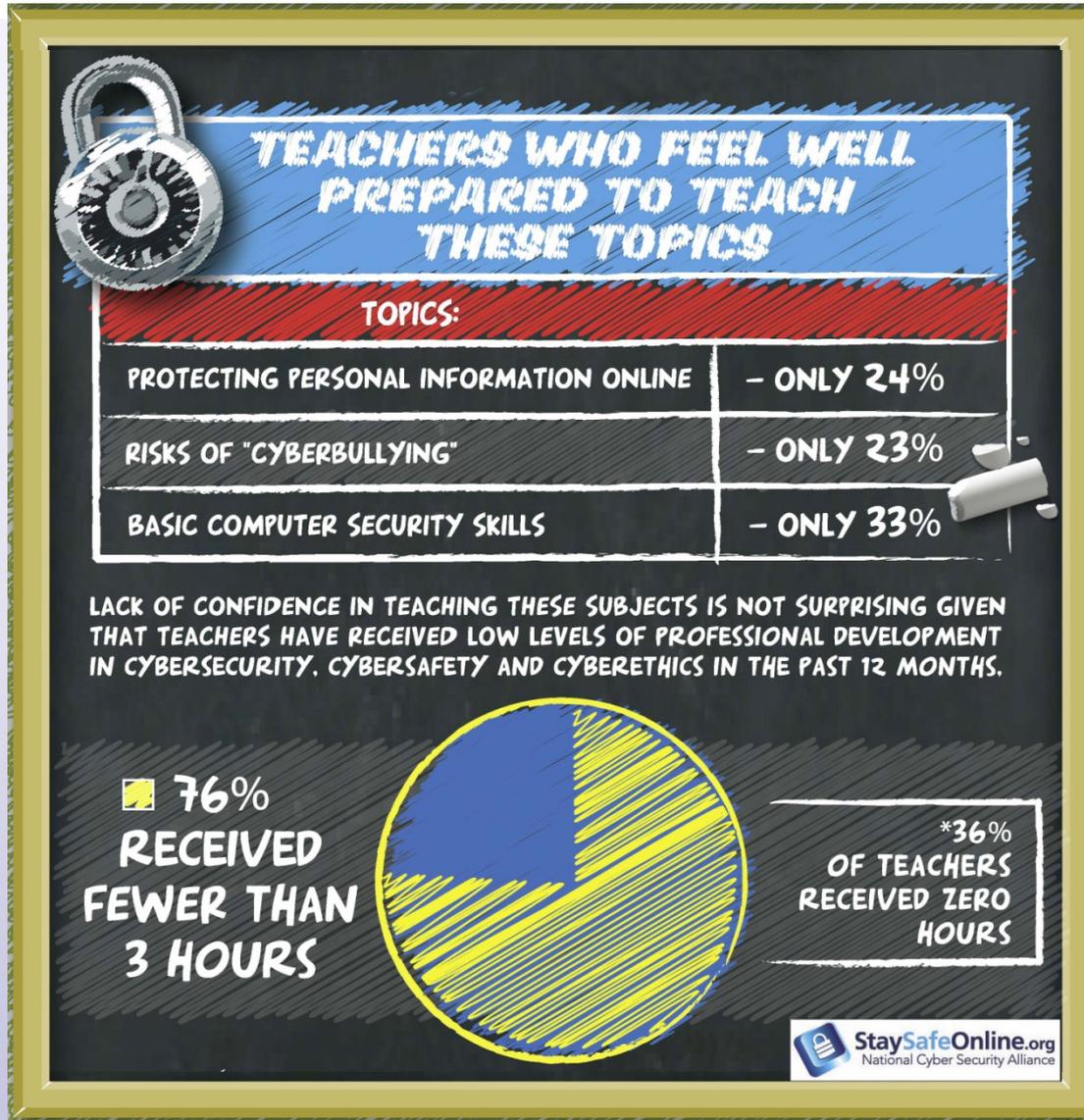
WHICH OF THE FOLLOWING HAVE YOU TAUGHT IN THE LAST 12 MONTHS?

TOPICS RELATED TO:

ONLINE SECURITY	23% - STRONG PASSWORDS	19% - PEER-PEER NETWORK RISKS
ONLINE SAFETY	18% - SOCIAL ENGINEERING & SCAMS	34% - SHARING PERSONAL INFORMATION ONLINE
ONLINE ETHICS	33% - RESPECTING PRIVACY	15% - DEALING WITH HATE SPEECH ONLINE



"Our K-12 students are more oriented with the digital atmosphere than ever before," said **Pamela Warren**, **cybercrime strategist and director of global public sector and critical infrastructure initiatives for McAfee**. "It's important to start arming them with smart resources to protect themselves online from the beginning of the formal education process and to continue reinforcing those messages throughout their K-12 experience. We're proud to collaborate with NCSA and CyberSmart! Education to prepare students for security and online safety both in and beyond the classroom setting."



2012 National Consumer Online Safety Study

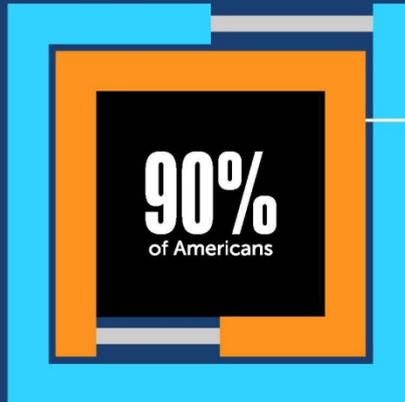


- The National Cyber Security Alliance conducted a new study with McAfee to analyze the cyber security behaviors and perceptions of Americans.
- The study was conducted by Zogby Analytics, which surveyed 1,000 adults nationwide from August 31, 2012 to September 3, 2012 - MOE +/- 3.2 percentage points.

WHY PROTECTING THE INTERNET IS A SHARED RESPONSIBILITY

THE INTERNET IS VITAL TO OUR ECONOMY AND OUR DAILY LIVES

Sponsored by



- BELIEVE A SAFE AND SECURE INTERNET IS CRUCIAL TO OUR NATION'S ECONOMIC SECURITY
- YET DO NOT FEEL COMPLETELY SAFE FROM VIRUSES, MALWARE AND HACKERS WHILE ON THE INTERNET

Here are some ways that Americans rely on the Web:



Use their smartphones to access the Internet.



Have jobs that depend on a safe and secure Internet (32% of which say their job is very dependent).



Believe losing the Internet on the job for 48 straight hours is disruptive and/or extremely disruptive.

“The Internet is central to our daily lives and our economy and this new survey shows that the overwhelming majority of Americans believe keeping this system safe and secure is vital,” **said Michael Kaiser, executive director of the National Cyber Security Alliance.** “The Internet is a shared resource for so many of our daily activities which is why protecting it is a shared responsibility. **We advise every computer user to STOP. THINK. CONNECT.**”

WE CAN ALL DO MORE TO STAY SAFE ONLINE

Sponsored by



STRONG PASSWORDS ARE THE FIRST KEY TO ONLINE SAFETY, BUT SOME OF US HAVE NEVER CHANGED PASSWORDS TO:



26%

Were notified that their personally identifiable information (e.g. password, credit card number, email address) was lost or compromised because of a data breach in the last year.



40%

Of all targeted cyber attacks are directed at companies with less than 500 employees.



58%

Decided not to download an app to their smartphone over a privacy concern.

**We are only as strong as the weakest link on any network.
The Internet is a shared resource, protecting it is a shared responsibility.**

"The threat to the safety of Americans online is growing every day and as the survey shows the fear of Americans has also grown to 90 percent," **said Gary Davis, vice president of global consumer marketing at McAfee.** "It is our responsibility to make sure that consumers are aware of these growing threats so they can be best prepared to defend themselves against these hidden criminals."

2012 National Investors Study



Cybersecurity Directly Affects Investor Attitudes, New HBGary Survey Finds

Survey Reveals Investors Demand More Transparency About Corporate Cyberattacks

- Zogby Analytics was commissioned by HBGary, a subsidiary of ManTech International Corporation, to conduct an online survey of 405 adults (+/- 5% margin of error) in the US that identified themselves as part of the Investor Class conducted in February 2013

- "For some time, we have said that cybersecurity cannot be a "checkbox" item on a company's operational to do list," **said Ken Silva, senior vice president of cyber strategy for ManTech's Mission Cyber & Intelligence Solutions Group.** "This survey proves that today's investors are more educated about the damage cyberattacks can cause to a company's brand and financial bottom line. The high cost of cyberattacks cannot be understated."

- **67% of Investors are likely to research whether the company has ever been fined or sanctioned for previous cybersecurity incidents**
- **71% of Investors are likely to use the Cyber security history of a company when deciding whether to invest if it is included in regulatory filings**
- **68% of Investors are unlikely to invest in a company that had a history of one or more cyber attacks**

- "Consumer data breaches grab the headlines and the large liability settlements. But the lack of concern for IP theft, underscores the need for broader education about the financial risk IP theft poses to a company" **said Jim Butterworth, HBGary chief security officer.** "The pilfering of American company trade secrets and other sensitive data is happening every day - costing our corporations billions of dollars in lost revenue."

2012 National Small Business Study



- The National Cyber Security Alliance conducted a new study with Symantec to analyze cybersecurity practices, behaviors and perceptions of small businesses (less than 250 employees) throughout the United States.
- Zogby Analytics conducted the study from September 27 - September 29, 2012. The survey had a MOE +/- 3.1 percentage points.

AMERICA'S SMALL BUSINESSES MUST TAKE ONLINE SECURITY MORE SERIOUSLY

SMALL BUSINESSES FORM BACKBONE OF U.S. ECONOMY

Sponsored by



1 IN 2 AMERICAN
WORKERS ARE
EMPLOYED IN A
SMALL BUSINESS



15 MILLION
NET NEW JOBS
CREATED BETWEEN
1993 AND 2009

- "We want U.S. small businesses to understand they cannot completely remain safe from cyber threats if they do not take the necessary precautions," **said Michael Kaiser, executive director of the National Cyber Security Alliance.** "A data breach or hacking incident can really harm SMBs and unfortunately lead to a lack of trust from consumers, partners and suppliers. Small businesses must make plans to protect their businesses from cyber threats and help employees stay safe online."

THE INTERNET IS A CRITICAL RESOURCE FOR U.S. SMALL BUSINESSES



SAY A SAFE AND TRUSTED INTERNET IS CRITICAL TO THEIR SUCCESS



Have one or more employees who use the Internet for daily operations

Say that the loss of Internet access for 48 straight hours during a regular business week would be disruptive to their business—38% say it would be extremely disruptive



A CYBER SECURITY DISCONNECT: MAJORITY OF U.S. SMALL BUSINESSES SATISFIED WITH THEIR ONLINE SAFETY MEASURES...



77% say their company is safe from cyber threats such as hackers, viruses, malware or a cyber-security breach

66% say they are not concerned about external threats (like a hacker or cyber-criminal stealing data) or an internal threat (like an employee, ex-employee or contractor/consultant stealing data)

47% believe a data breach incident would have no impact on their business and it would be treated as an isolated incident

18% say they would not know if their computer network was compromised

Sponsored by



YET MOST U.S. SMALL BUSINESSES CAN IMPROVE THEIR ONLINE SECURITY PRACTICES

Sponsored by
NATIONAL
CYBERSECURITY
ALLIANCE



87% nearly 9 in 10 do not have a formal written Internet security policy for employees



69% do not have even an informal Internet security policy for employees



59% do not have a contingency plan outlining procedures for responding and reporting data breach losses



75% do not have policies for employee social media use on the job while 23% have established policies



60% do not have a privacy policy that employees must comply with when they handle customer or employee information

"It's **terrifying** that the majority of U.S. small businesses believe their information is protected, yet so many do not have the required policies or protection in place to remain safe," **said Brian Burch, vice president of Americas Marketing for SMB, at Symantec.** "Almost 40 percent of the over 1 billion cyberattacks Symantec prevented in the first three months of 2012 targeted companies with less than 500 employees. **And for the small, poorly protected companies that suffer an attack, it's often fatal to their business."**

Q&A

The intersection of Cyber Security and Public Opinion:

Consumers ~ Teachers
SMB Owners ~ Investors

Zogby
Analytics

John Zogby, Senior Analyst, Zogby Analytics
zogbyanalytics.com

