2012 NATIONAL ONLINE SAFETY STUDY

The National Cyber Security Alliance has conducted a new study with McAfee to analyze the cyber security behaviors and perceptions of Americans. The study was conducted by JZ Analytics, which surveyed 1,000 adults nationwide from August 31, 2012 to September 3, 2012. Slight weights were added to age, race, gender, region, party, education, and religion to more accurately reflect the population. The margin of error is +/- 3.2 percentage points. Margins of error are higher in sub-groups. Key findings of this study are listed below.

GENERAL CYBER SECURITY PREPAREDNESS

- Majority of American's agree that a safe and secure Internet is crucial to our nation's economic security (90%).
- At the same time, an equal amount of American's do not feel completely safe from viruses, malware and hackers while on the Internet (90%)
- Respondents are most concerned about identity theft while on the Internet (41%); 16% getting infected with malware or a virus; 13% someone hacking into their financial information (or their family's); 5% loss of privacy; 4% someone monitoring or recording their online account activity; 3% concerned about a cyber criminal gaining information about them or their family; 4% worried about falling victim to an online scam or fraud; and 3% worried about someone hacking their online connections or network.

HOW AMERICANS STORE DATA

- Storing Digitally: 26% store their banking information on their desktop/laptop; 6% on their smartphone; 4% on tablet and 2% on a cloud service. Twenty-four percent store personal records on desktop/laptop vs. 7% on smartphones. Twelve percent store business records on their desktop/laptop. Overall, the main things people store across all platforms are digital photos and music, and it is clear that people feel much more comfortable storing a wide array of digital information on desktops/laptops vs. smartphones, tablets and cloud services.

PASSWORD PROTECTION MATTERS

- Most people say they have changed the password on a major online account without being prompted to do so by their service provider sometime in the past six months (23%) or 14% in the last year, 13% in last week, and 23% in the past month. Seventeen percent have never changed their passwords.
- For social media users, 49% have changed their passwords once or more this past year, with 6% changing passwords weekly. At the same time, 42% have never changed their social media passwords.

- Sixty-one percent of respondents changed their online banking account passwords at least once a year while 28% have never changed their passwords.

PARENTS AND CYBER SAFETY

- Of those respondents with children, parents are most worried about them coming across adult sexual content/pornography (39%) followed by having contact with strangers when they are online (27%). Ten percent are worried about bullying or harassment from peers; 9% about identify theft; 3% concerned about portrayals of drug or alcohol use; 2% long-term damage to their reputation.

AGE APPROPRIATE FOR DIFFERENT TECHNOLOGIES

- People think that it is appropriate for children 10-16 to own a tablet (46%) or smartphone (53%) 10-13 year-olds to own a desktop/laptop (30%) and 7-9 year-olds (18%), 14-16 year-olds to have a social network account (31%), and 10-13 year-olds to have an email account (29%).

HOW AMERICANS CONNECT

- Sixty-one percent of American's feel safest accessing the Internet using a laptop or desktop; 9% using a smartphone and 3% using a tablet. (22% have only ever accessed the Internet using a desktop/laptop.)
- Most respondents think that connecting to an unsecured wireless network puts them most at risk of a cyber crime or loss of personal information (30%), followed by not having any or enough security software (22%); 13% said public computer (such as at hotel); 12% said not knowing how to identify if a site is secure; 7% said not having strong passwords and 3% said not updating other software (such as browser or operating system).

SMARTPHONES/MOBILE

- About half (49%) use their smartphones to access the Internet, but roughly the same amount (41%) say they do not own such a device.
- Sixty-four percent feel their smartphones are safe from hackers, malware or other cybercrimes, with 15% of those respondents feeling very safe. At the same time, 29% do not feel their smartphones are safe.
- Although the amount of smartphone users continues to rapidly increase, 58% of current users have never backed up their devices by storing the information or data elsewhere.
- Many respondents are not taking additional security precautions to protect their smartphones with over three-fifths (64%) having never installed security software or apps on their device in order to make it more secure from viruses or malware.
- Nearly half of respondents (44%) feel more cautious when accessing the Internet on a smartphone than from a desktop or laptop.

- Fifty-eight percent of respondents decided not to download an app to their smartphone over a privacy concern. Of those who did not download an app, many were concerned most about potential identity theft (55%), privacy issues (50%), were unsure about how their data would be collected and used (48%), and/or were concerned about the reputation of the app developer/service provider (40%).
- Sixty-nine percent of respondents were concerned about the basic security of their smartphone, tablet or laptop and what could happen if it gets lost.
- In the last six months, smartphone owners have most frequently kept a list of personal contacts (57%), stored photos (68%), conducted social networking (57%), and kept a calendar (45%) on their device, and/or instant messaged someone (43%). Twenty-nine percent researched potential purchases; 22% accessed work emails; 33% conducted mobile banking; 27% shopped; 12% stored documents; 26% made online payments; 8% accessed work documents or databases on a server; 7% purchased good from an auction site.

CYBER VICTIMS

- Seventeen percent (17%) say they have been the victim of a crime that was committed over the Internet such as identity theft, data theft, bullying or auction fraud, and 29% say they know someone who has been a victim of such crimes (64% do not).

THOSE EMPLOYED

- Of those who are employed, roughly half (48%) were allowed to use a personal tablet, smartphone or laptop to perform job functions while 31% connected to their work network using these personal devices.
- Forty-two percent of employed respondents say their employer has a formal policy, training, or security requirement they must follow. At the same time, 44% of respondents said their employers do not have guidelines.
- Fifty-nine percent say that their job is dependent on a safe and secure Internet, 32% of which say it is very dependent.
- Over three-quarters (78%) say that losing Internet access at their job for 48 consecutive hours during a regular business week would be disruptive, 33% of which say it would be extremely disruptive.

INTERNET SERVICE PROVIDER

- One in four respondents (26%) say their personal data was put at risk in the last year and were notified by a business, online service provider or organization that their personally identifiable information (e.g. password, credit card number, email address, etc.) was lost or compromised because of a data breach.
- A majority of respondents (86%) agree that they would want to be notified if a trusted third party such as an Internet service provider (ISP), financial

institution, e-commerce site or online service provider knew that their computer was infected with a virus or malware. With 66% strongly agreeing.

- Respondents think that the Internet service provider is most responsible for providing information on how to stay safe and secure online (31%), followed by security software providers (29%) and companies they do business with online (10%) and 9% thought federal government.