AN INDEPENDENT SUPPLEMENT BY MEDIAPLANET TO USA TODAY

No.3/October 2012

MEDIA PLANET

CYBERSECURITY

Safe money Bank on these mobile security tactics

Identity theft survey Test your knowledge

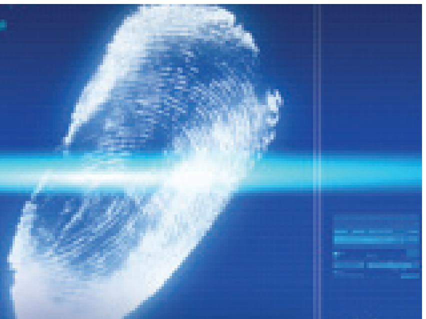
Job security Information security is a booming industry

2 FACTS ABOUT AMERICA'S INTERNET USE

DEFENDING THE NATION, SECURING THE FUTURE

United States Army General Keith B. Alexander discusses defending the nation against cyber threats

PHOTO: NSA



CHALLENGES

During October and every day all year long, we encourage you to **take security measures,** understand the consequences of your actions online and enjoy the benefits of the Internet.

FACT 1

17% OF ONLINE USERS HAVE NEVER CHANGED A MAJOR ONLINE ACCOUNT PASSWORD WITHOUT BEING PROMPTED

A shared responsibility

October is a time of changing leaves and crisp air. It's also the ninth annual National Cyber Security Awareness Month, a nationally coordinated effort by government, industry, nonprofits and individuals to make Americans aware of how to stay safer and more secure online.

Our recent National Cyber Security Alliance (NCSA) research shows that 90 percent of Americans believe that a safe and secure Internet is vital to our economic security and nearly 6 in 10 say their jobs are dependent on it. At the same time, 90 percent do not feel completely safe from viruses, malware and hackers while on the Internet.

Beyond the economic importance of the Internet, most Americans now count on a reliable and trusted Internet as an integral part of their daily lives. Whether it's engaging in ecommerce, connecting with family and friends, or participating in communities, we expect to be able to safely go online at anytime from anyplace.

We can only achieve a safer and more secure Internet if everyone does his or her part. That's why the theme for National Cyber Security Awareness Month is "Our Shared Responsibility," because the Internet is shared resource and protecting it is our collective duty.

We can all do more to protect ourselves but learning good online safety starts with three easy steps: STOP. THINK. CONNECT.

- **Stop:** Before going online, take time to understand and reduce your risks.
- **Think:** Take a moment to be certain the path ahead is clear. Watch for warning signs and consider the consequences of your actions and behaviors on you and others.

Michael Kaiser
Executive Director,
National Cyber
Security Alliance

BEST TIPS

- Keep a clean machine: The latest security software, web browser, and operating system are best defenses against cyber threats.
- Make passwords long and strong: Combine capital/lowercase letters with numbers/symbols to create a more secure password.
- When in doubt, throw out: Delete or mark as junk if an email, social media post or online ad looks suspicious.

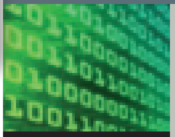
- **Connect:** Enjoy the benefits of the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself, your family and your computer.

Those three simple steps take just moments and form the foundation of a safe and healthy online experience. It's a message that can be taught by anyone and will make us all safer online.

Each year our lives become more dependent on the Internet. That increasing reliance on this shared resource makes what we do to stay safe even more critical. There is an added benefit as well. Every step an individual takes to stay safer online—such as keeping a clean machine free from from viruses and infections—makes the Internet more secure for everyone.

MICHAEL KAISER
editorial@mediaplanet.com

WE RECOMMEND



PAGE 7

The importance of protection in the workplace

MEDIA PLANET

CYBERSECURITY, THIRD EDITION, OCTOBER 2012

Publisher: Kelly Lehmkuhl
kelly.lehmkuhl@mediaplanet.com
Business Developer: Ian Silbert
ian.silbert@mediaplanet.com
Designer: Sarah Davidson
Managing Director: Luciana Colapinto
luciana.colapinto@mediaplanet.com
Editorial Manager: Sara Quigley
sara.quigley@mediaplanet.com

Contributors: General Keith B. Alexander, Jacqueline Beauchere, Rowland Johnson, Michael Kaiser, Stephen Orenberg, Cindy Riley, Wendy Taylor

Distributed within:
USA Today, October 2012
This section was created by Mediaplanet and did not involve USA Today or its Editorial Departments.

FOLLOW US ON FACEBOOK & TWITTER!
facebook.com/MediaplanetUSA
twitter.com/MediaplanetUSA

Mediaplanet's business is to create new customers for our advertisers by providing readers with high-quality editorial content that motivates them to act.

Don't put your private life on display.

Microsoft

National Cyber Security Awareness Month

In October and all year long, take extra steps to avoid Internet scams and identity theft.

Be defensive with sensitive information

- Avoid sharing it in email, instant (IM) or text messages. They may not be secure.
- Save banking, shopping, and other financial transactions for your secured home connection.
- Before entering sensitive info, look for signs a webpage is secure: "http**s**" in the address and a closed padlock.

Boost your computer's security

- Keep all software (including your browser) current with automatic updating. Install legitimate antivirus and antispyware software.
- Protect your wireless router with a password, and use flash drives cautiously.
- Think before you click links or call a number in a message, even if you know the sender. If you're unsure, make contact on a different device or account.

Create strong passwords or phrases

- Mix capital and lowercase letters, numbers, and symbols; keep them secret.
- Don't reuse passwords.

Watch out for scams

- Be wary of alarmist messages with urgent requests for personal information.
- Look out for misspellings and grammatical errors, or deals and prizes that sound too good to be true.

For more tips on protecting your information, family and devices:

Microsoft.com/Security
Facebook.com/SaferOnline
Twitter.com/Safer_Online
YouTube.com/MSFTOnlineSafety

STOP | THINK | CONNECT™

BEST TIPS

PHOTO: SXC.HU

Keep your money safe from cybercriminals

Ensure the safety of your credit card information and financial data when you're banking and shopping online. Follow these helpful tips to keep your money safe.

→ Make sure the website you are on is legitimate—more than 5,000 infected websites are detected every day.

→ Run frequent checks of your PC for vulnerable software—more than 125,000 new malware samples are detected every day.

→ Don't be fooled by phishing emails—more than 70 percent of all phishing emails directly target your money.

→ Ensure your passwords and the data you enter online cannot be tracked by a keylogger—use a secure keyboard for entering all of your personal data online.

editorial@mediaplanet.com

PANEL OF EXPERTS

	Question 1: Why is cybersecurity such a problem?	**Question 2:** Is it necessary to protect your smart phone or tablet?	**Question 3:** What is the biggest mistake Americans make regarding cybersecurity?
 Stephen Orenberg President, Kaspersky Lab North America	**Three reasons:** there are new kinds of threats besides just computer viruses, there are more devices we use that are at risk, and we are doing more things online that expose us to risk. Activities ranging from people paying their bills to shopping for anything from concert tickets to TVs have become the norm, rather than the exception.	**Absolutely.** That device in your pocket used for texts, emails and going online has more computing power than most PCs had five years ago. Cybersecurity is all about protecting the information accessed on the device. Installing a banking app on your phone or tablet, for example, creates another connection to your money that cybercriminals can try to exploit.	**Probably it's the mindset** that "it can't happen to me." Cybercriminals cast wide nets and we're all vulnerable unless we have the proper defenses installed on our devices. Consumers and businesses want to be safe but often fail to take the proper steps to protect themselves.
 Jacqueline Beauchere Director, Microsoft Trustworthy Computing	**The goal of cyber criminals** and their scams are to collect your personal or company's information, or money—or both. We all play a part in helping to keep the Internet a safer place. Taking a moment to stop and think before clicking on links, opening photos, or other attachments, might save you a lot of trouble from downloading malicious software that could destroy your device or company's network.	**It's necessary to protect** all devices that connect to the Internet. Treating all public wireless connections and Wi-Fi hotspots as a security risk is a good idea because they are often unsecured. Criminals can use inexpensive and readily available devices to "look" at the traffic that passes through these unsecure connections. Watch out for mock Wi-Fi hotspots that may expose your device to a hacker who could take control of it.	**People have come** to rely on the technologies that keep pace with their digital lifestyles. Three simple habits to help avoid many of the online safety pitfalls are: (1) keeping passwords and PINs private,(2) not storing these on your mobile device, and (3) keeping all software (including your browser) current with automatic updating.

A critical eye: The first line of scam defense

As online scams shift from technical to social, Internet con artists are becoming more creative and sophisticated in gaining access to personal information, stealing money and impersonating unsuspecting victims.

To prevent falling prey to lottery schemes, phishing ploys and fake anti-virus alerts, it's crucial to view all emails and links with a critical eye, according to a new Microsoft Scam Defense Survey.

"If you have even the slightest doubt about an email or a website's legitimacy, play it safe and leave," cautions Jacqueline Beauchere, Director, Trustworthy Computing, Microsoft Corporation. "We see the Scam Defense Survey as a vehicle to further encourage individuals and families to take action and to help them safeguard their digital lifestyles."

Microsoft's approach to online protection includes technological tools, education and guidance and partnerships with government, industry, law enforcement and other organizations, to help create safer, more trusted computing experiences. The report finds adults in the U.S. have encountered approximately eight different types of online scams. Sixty-two percent of respondents feel they're unlikely to become a victim of online fraud, but only 12 percent say they feel fully protected. Most worry about fraudulent websites, identity theft and work-from-home offers.

Consumers should guard sensitive information by refusing to share it via email or instant and text messages. Complete banking other financial transactions using home computers only. Before entering personal information, look for signs a webpage is secure, with "https" in the address and a closed padlock. Notifications that recipients are featured in newly uploaded social media photographs should also be met with skepticism.

All software, including browsers, should be kept current with automatic updating. Protect wireless routers with passwords and use flash drives cautiously. Create strong passwords that are secret and not reused. An urgent message requesting personal information is another red flag.

Adds Beauchere, "If you have even the slightest doubt about an email or a website's legitimacy, play it safe and leave."

CINDY RILEY

editorial@mediaplanet.com

NQ Family Guardian™

Smartphone protection for kids. Peace of mind for parents.

Who says smartphones and kids don't mix? With strong security and privacy protection, parents can say goodbye to those nagging fears and hand over that smartphone.

NQ Family Guardian™ eliminates the fear factor for parents by allowing them to monitor their kids' smartphone activities and location.

- *Get smartphone safety tips and tools for the whole family at: www.nqmobilefamily.com*
- *Try NQ Family Guardian for free: www.nq.com/familyguardian*

NQ mobile
Safeguarding your mobile world

NATIONAL CYBERSECURITY ALLIANCE

NQ Mobile™ is proud to be a National Cyber Security Awareness Month Champion.

A COMBINED DEFENSE: PUBLIC-PRIVATE PARTNERSHIP AGAINST CYBER ATTACK

When recently asked to rate from one to ten how prepared the nation is for a serious cyber attack on infrastructure, Gen. Keith B. Alexander—Commander, U.S. Cyber Command/Director, National Security Agency/Chief, Central Security Service—offered an astonishing response: "three."

Alexander doesn't sugarcoat the need to address potential risks to public and private systems, whether from criminals, rogue states or non-state supported threats, such as terrorists.

"I think [in] the next generation [there] are going to be destructive attacks," Alexander said. "I think we're always going to see people out there [who] try to exploit for crime. I think we're going to see people trying to exploit for intelligence. What concerns me is when somebody jumps into a series of mobile devices, and then throws an attack against one of our critical infrastructure key resources—now we've got a problem."

Alexander's greatest unease is the country's current inability to simultaneously detect malicious cyber activity in both the public and private sectors, as well as a lack of response standards.

Preventing attacks

The solution in Gen. Alexander's opinion as well as many of his Washington, D.C., counterparts relies on enhancing the ability to see an attack anywhere within the U.S., increasing the protection of critical systems and better educating every system operator, from military to small businesses.

While the Cyber Security Act of 2012—bipartisan legislation designed to bridge communication between government and industry—died in the senate this summer due to privacy and government overreach concerns, the Obama administration has signaled plans to resurrect at least parts of the bill through executive order this year.

And while government officials continue working on details of how private and public sectors can work together, one area Alexander seems clear on is the need for increased training throughout government and businesses.

"We have over a hundred universities that are doing information assurance, cyber security-related stuff," Alexander said. "Take the best of that and put it on the table, and that's how we've got to educate our future force."

Between rapid technological advancements of smartphones and information circumnavigating the globe in approximately 133 milliseconds, Alexander warns there isn't much time to waste before setting plans and protocols.

"The industry can't do it by itself," he said. "Government can't do it by itself. If we don't operate as a team, it's not going to happen."

WENDY TAYLOR
editorial@mediaplanet.com

PHOTO: NSA

Secure information, secure employment

Q: What can this growing industry provide other than online safety?
A: Job creation and opportunity.

These days, an industry with low unemployment seems rare. Statistically non-existent unemployment sounds impossible. But according to the U.S. Bureau of Labor Statistics' most recent survey, none of those identifying themselves as an information security analyst were unemployed—a consistency since January 2011.

With increasing demand for both government and private-sector jobs within cybersecurity, it's only natural that education and training programs are also experiencing huge growth.

Wide-open field

Dr. Jennifer Bayuk, a private cybersecurity consultant, as well as a professor and director of systems security engineering at Steven's Institute of Technology, says part of the field's opportunity falls within its broad needs—from very controlled and strict data entry to process design, security testing, engineering and regulatory compliance.

"Information security is a pretty large field, with a wide variety of types of positions in it," Bayuk said, agreeing that education within the industry ranges from those exiting high school to researchers holding doctorate degrees.

A step ahead

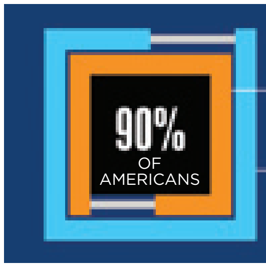
Bayuk feels good cybersecurity professionals must hold a unique combination of fearlessness and a bit of paranoia.

"It's very easy to see what the adversary did and then patch your systems to make them less vulnerable to an attack that's already in the newspaper," she said. "The job for a good security professional is to anticipate those abuse cases before someone tries to do them."

And as education and training programs from technical to the collegiate level expand to keep up with the rapid pace of the relatively young, 40-year-old industry, the approach to training focuses not only on technological and procedural information, but logic and problem-solving skills.

"This mirrors IT in general," Bayuk said. "You shouldn't be teaching anybody today's technology. You should be teaching them to think about technology because the technology that they will be working on we can't even envision yet."

WENDY TAYLOR
editorial@mediaplanet.com



BELIEVE A SAFE AND SECURE INTERNET IS CRUCIAL TO OUR NATION'S ECONOMIC SECURITY

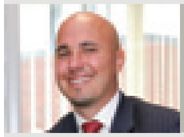
YET DO NOT FEEL COMPLETELY SAFE FROM VIRUSES, MALWARE AND HACKERS WHILE ON THE INTERNET

SOURCE: NCSA

Q & A

FACT 2

59% OF AMERICANS HAVE JOBS THAT DEPEND ON A SAFE AND SECURE INTERNET (32% OF WHICH SAY THEIR JOB IS VERY DEPENDENT)



Rowland Johnson
CEO, Nettitude Inc.

What is happening in the current cybersecurity landscape?

2012 has seen some significant exposures in core desktop applications, which leave home users susceptible to data breach. In the corporate world, we have seen assaults become more sophisticated, and hackers are now using targeted information collected from social media. With the continued growth of mobile and tablet technology, we expect to see increased vulnerabilities in mobile applications.

Why is it important to take the threat seriously?

This isn't just a problem for large corporate and government agencies; attacks are taking place every day, in all types of American companies.

What can organizations do to protect themselves and their customers?

Security isn't just about software or hardware products. We find that most organizations that are hacked have firewalls and other security technology. They just aren't configured effectively, and the users that interact with them don't have appropriate security training.

What can be done to prepare for wider security challenges?

Security training and security awareness should be high on everyone's agenda - people are frequently the weakest link in the chain. Until we can educate users on how to practice strong security techniques, hackers will still continue to compromise organizations and steal data.

editorial@mediaplanet.com

My favorite things.
They matter to me,
so I protect them.

Paul - Restaurant Critic

Safeguarding Me

My photos, private letters and passwords are all on my laptop, so I protect them with Kaspersky. So do 300 million others worldwide.

usa.kaspersky.com/paul

amazon.com · BEST BUY · Fry's Electronics · Office Depot · OfficeMax · Sam's Club · STAPLES that was easy · TARGET · Walmart Save money. Live better.