DIGITAL SECURITY

Featuring

TECH SAVVY KIDS
How young is too young?

SMALL BUSINESSES
Six pillars of protection

CATCH HIM IF YOU CAN

From global con artist to renowned security consultant, the infamous Frank Abagnale, Jr. explains how to be safe in the digital world.

nuspire networks

CONNECTING THE DOTS
IN ENTERPRISE SECURITY OPERATIONS

GLOBAL LEADER IN DISTRIBUTED ENTERPRISE SECURITY

www.nuspire.com/usatoday
October is National Cyber Security Awareness Month and a good time to remember that all of us play a role in making the Internet safer.

Securing our digital world

October is National Cyber Security Awareness Month, when we focus on a unifying theme of “Our Shared Responsibility,” to recognize the part we all play in being safer online and making the Internet more secure for everyone.

When last we polled Americans and small businesses on their attitudes about security, 90 percent said that a safe and secure Internet is vital to our nation's economic security, and nearly 60 percent said their jobs depended on it and 73 percent of small businesses told us that a safe and trusted Internet is critical or somewhat critical to their business.

But unfortunately our actions haven’t always reflected our awareness of the importance of Internet security. Our newest poll shows that a large percentage of Americans still aren’t taking some of the simplest steps available to make themselves — and the Internet itself — safer.

Preventing digital threats

Too many of us still use only one or two passwords across all of our online accounts, and far too many of us keep the same passwords for months on end, rather than making regular changes.

Many of us still don’t use a password or pin to protect our mobile devices. Maintaining long, strong, and unique passwords is just one example of a simple, non-technical practice that can have a huge impact on Internet safety.

For all of the media focus on distant cyber attacks, mysterious hackers and scary-sounding computer viruses, the simple truth remains that each of us possesses great power to prevent the vast majority of online threats from harming us. And if we all were to exercise that power, the global effect on Internet security would be profoundly positive.

Tapping into that power is as simple as three words: STOP. THINK. CONNECT.

Stop. Make sure you have taken safety and security precautions, such as running up to date software.

Think. About the potential consequences of your actions and behaviors.

Connect. With more confidence knowing that you’ve taken steps to protect yourself and your family and enjoy the Internet.

The power is in your hands.

This October, I urge you to use it.

MICHAEL KAISER
executive@mediaplanet.com

Michael Kaiser
Executive Director, National Cyber Security Alliance

91% of adults are now using cell phones

28% used mobile banking in the past 12 months
THEY’RE NOT SO CYBER THREATENING WHEN YOU SEE THEM COMING

Compromised networks and data can bring your mission to a halt. So don’t compromise on security. Lockheed Martin’s proactive, intelligence-driven approach has thwarted advanced persistent threats for more than a decade. Further securing our position as the #1 provider of I.T. solutions to the federal government. Learn about security that doesn’t compromise at www.lockheードmartin.com/cyber.
Survey results are in
Children these days are growing up surrounded by new technologies. The question isn’t if parents should allow their kids to use online devices, but when?

According to a new survey by Microsoft, titled “How Old Is Too Young?,” 94 percent of all parents allow their kids to use at least one online service or device. The survey also found that the average age at which parents allow children to use devices independently is eight years old.

Additionally, 29 percent of parents allow their children to use mobile phones unsupervised, while 40 percent allow their children to use a computer unsupervised. In total, 41 percent of parents allow their kids to use a gaming console unsupervised.

“It’s never too early—or too late—to talk to your kids about being safer, smarter, and more considerate online,” said Jacqueline Beauchere, Chief Online Safety Officer at Microsoft. “While kids may be savvier about how the devices work, parents can be instrumental in helping to shape how kids think about, engage with, and generally behave with technology both online and off.”

Below are tips for parents on how to start or continue the online safety conversation, with the goal to engage educate, enforce and evaluate the best rules for your family: Parents should help children choose apps that are appropriate for their age and maturity. It’s important to use and buy apps that are well-reviewed and from a reputable source.

Once kids start signing up for social networking sites, parents should help them make their profiles private and also ask them to think twice about who they accept as friends.

Finally, parents should talk to their children about promoting a positive image online and being respectful of others when posting comments. It’s important to come together and explore the games kids want to play and create family guidelines for their use.

MARY ANN GEORGANTOPOULOS
editorial@mediaplanet.com

FOR THE COMMON GOOD

Frank Abagnale, Jr. has come a long way. Between the ages of 16 and 21, he posed as an airline pilot, an attorney, a college professor and a pediatrician while cashing $2.5 million in fraudulent checks in every state and 26 countries.

After serving time in France, Sweden, and the United States, Abagnale was offered a position working with the FBI to investigate document fraud. Today, Abagnale is one of the world’s foremost authorities on forgery, embezzlement, and secure documents continuing to collaborate with the FBI for the past 37 years.

Securing your identity
“Me stealing your identity is like asking me to count to three,” he said. “It’s that simple.” Abagnale offers three tips anyone can do to protect their privacy and identity.

First off, he suggests purchasing a proper shredder. There are three different types of shredders, he says, but the ones most people use are ‘worthless.’ Documents shredded using a strip-cut shredder or cross-cut shredder can be put back together in an FBI lab in a matter of hours. Abagnale stressed the importance of buying a “security micro cut shredder,” which turns paper into confetti.

Secondly, Abagnale explains, when picking a credit monitoring service it is important to vet them and ask two basic questions. First, ask if they monitor all three credit bureaus. Second, ask if they notify you in real time. “When someone’s at Macy’s buying something in my name, I want my cell phone to go off right then so I can be proactive,” he said.

Finally, Abagnale does not use a debit card, which he calls “the worst financial tool that’s been developed.” The safest form of payment is a credit card. Every day he spends the credit card company’s money while his money is in a money market account collecting interest.

“If someone gets my number and charges $1 million on my credit card, by federal law I have no liability,” he said. “When I pay my bill every month, my credit score goes up. Every time you use a debit card, you expose your money and you get nothing in return.”

Abagnale has come a long way since his check fraud days. As the subject of a book, movie (“Catch Me If You Can” starring Leonardo DiCaprio), and play, Abagnale is in the perfect position to use his experience for the common good.

“Technology has made what I did, a thousand times easier,” Abagnale warns, a constant reminder to guard your digital information closely.

MARY ANN GEORGANTOPOULOS
editorial@mediaplanet.com

Have you started the “e-talk” with kids?

Is it time?

83% of parents who allow their child unsupervised access to a device or online service, also set rules or had a conversation about tech safety.

Two-thirds of those parents did so before kids reach age 10.

Microsoft
INTRODUCING METLIFE DEFENDER™
PROTECTION FOR YOUR FAMILY’S DIGITAL LIVES.

The company you trust is now here to protect your family online. With MetLife Defender you have a comprehensive security solution that monitors, detects and guards against digital threats.

- **Protection for your kids** — Unique apps and patented technology to defend against online predators, cyberbullies and child ID theft
- **Protection for your personal data** — Multi-layered defense that monitors your credit, safeguards your financial and medical information and defends against ID theft
- **Dedicated support with a $5 million service guarantee** — Timely alerts, 24/7 customer service, plus up to $5 million to help recover ID theft losses

Defend yourself and your family. Visit metlifedefender.com

MetLife Defender services are subject to the Terms & Conditions of the Subscriber Agreement and Service Guarantee. To review, please visit www.metlifedefender.com.
© 2013 MetLife, Inc. PEANUTS © 2013 Peanuts Worldwide. L1013346356[exp1014][All States]
In a cyber-centric world, student engagement is crucial

As cyber systems and processes begin to dominate our global economy, a disturbing trend is emerging. The U.S. is no longer producing the workforce it needs to sustain its position as the most innovative economy on the planet. A 2008 Congressional Research Service study revealed that among 15-year-old students, the U.S. ranked 28th in math literacy and 24th in science literacy. Something needs to change if the U.S. is to maintain its position as the world becomes increasingly cyber-centric. We must ensure that our nation is producing the people we need in science, technology, engineering, and mathematics (STEM) fields.

The fact is, if we do not attract students to technical fields, later is too late to prepare them to enter a technical workforce. If a student hasn’t been drawn to STEM in his or her teen years, we will seldom shape their choices.

But how do we do that? How do we inspire and excite high school students to fields they often see as too difficult? Why should they move down the rocky STEM road (think calculus, physics, and thermodynamics) when much easier paths call them? The answer—I think—lies in the same innovation that has brought us what we have.

Educators, organizations, and government at all levels must identify the things that excite students. Nothing does that like competition. We must use the same focus, attention, and energy that draws 7 million high school students a year to sports to draw our students to STEM competitions. We must use the same ingredients to highlight the achievements of those who take on the challenges of robotics, science, and cyber competitions in our high schools.

American innovation has overcome nearly every challenge we have faced. We can use that same innovation to excite students to enter the rich and rewarding STEM fields that call them. A little team—and American—spirit can go a long way.

BERNARD SKOCH
THE AIR FORCE ASSOCIATION’S CYBERPATRIOT COMMISSIONER
editorial@mediaplanet.com

The six Pillars of Cyber Security Leadership

Every business owner, CEO or manager should be asking these six questions. Are you?

“We’re a small 5-person company that handles sensitive client data. I’m not confident that we’ve done all we should cyber security-wise.”
— John G., Small Business Owner

It’s a tricky situation. Smaller companies have to — and want to — protect sensitive information. But they don’t have the budgets, IT staff or compliance knowledge to master cyber security like their corporate cousins. They want to build a culture of security, but they don’t know where to start.

Just in time for Cyber Security Awareness Month, iKeepSafe has created the Six Pillars of Cyber Security Leadership to help small businesses ask the right questions, hire the right people and prevent cyber flare-ups despite their resource gaps.

MARSALI HANCOCK
PRESIDENT, CEO, INTERNET KEEP SAFE COALITION
editorial@mediaplanet.com

1. EXPOSURE IDENTIFICATION
How are we handling account management, data backup and cyber incidents?

2. BUSINESS COMPLIANCE
What are we doing to protect our valuable customer and vendor data?

3. PROPERTY PROTECTION
Will our business fold if we suffer a temporary or permanent loss of sensitive assets?

4. AGILITY PLANNING
What’s the game plan if we experience potential disasters such as a data breach or denial of service?

5. RISK MANAGEMENT
Do we have an employee who manages both information and physical security?

6. OPERATIONS POLICIES
Have we educated our staff around safe computing and data handling?
National Security Agency opens up

John DeLong, Director of Compliance at the National Security Agency (NSA), speaks out about the NSA regulations that have been a part of heated discussion for the nation. DeLong has devoted himself to educating Americans on the NSA’s role and their right to privacy, and he has also advocated for education within the cybersecurity industry.

Mediaplanet Many people have heard that NSA collects everything and anything — all around the world, including here in the USA. Many people claim that NSA violates privacy laws here at home. What's your response to such perceptions? John DeLong Perceptions are not the same as reality.

There are a lot of myths that are out there, a lot of perceptions. They’re somewhat pervasive, the NSA doesn’t set its own agendas, and it doesn’t act on its own authority. It (NSA) acts on permission from authorities. The requirements involved span all three branches of the federal government. The NSA permissions to operate are long. We don’t create the requirements under which we operate. Myth is not a great basis for any response.

MP Does NSA spy on Americans? JD One of NSA’s analysts, mathematician Roger Barkan, wrote an article and I think he said it best: “The NSA is not watching you, it’s being watched”. This idea that we’re spying on Americans is best answered by we’re not watching we’re being watched. And the second half of his phrase is how to watch the NSA, and I think that’s a very important discussion. All three branches have a role or a play a role in watching the NSA. They’re on the ground, they take reports, they ask questions. So I think the important question is: How can Americans watch the NSA? They’ll realize we’re focused on foreign targets, they’ll realize we’re a foreign intelligence agency. We don’t listen to average Americans, we don’t do what’s not been authorized.

Free ways to stay safe on your cell phone

Most of our daily activities involve a mobile device these days. That’s why you should take mobile security seriously and protect your phone and all information stored on it. Below are my best security tips and tricks which help you to stay safe on your device without spending a dime.

Anti-theft protection Every smartphone vendor offers free remote lock, wipe, locate features. “Find My iPhone” and “Android Device Manager” is a must on every device.

Screen lock protection A PIN or passcode is your first line of defense. Activate your device screen lock with a not so easy PIN or passphrase.

App store security Only download apps from your device’s official App Store, like Google Play, Apple App Store etc. Official App Stores filter all apps for virus and spyware.

Privacy Settings Hackers need to contact you before anything bad can happen. Never post your address, email, phone number on the web, social networks, craigslist etc.

1. What are some tips and tricks to help consumers avoid online risks?

Jacqueline Beauchere, Chief Online Safety Officer, Microsoft Corp.

Whether it’s sharing a special photo with a loved one or paying a bill online, remember to: 1. Save sensitive transactions for secured networks, not public Wi-Fi. 2. Look for signs that a webpage is secure — like using sites with https (the “s” stands for secure), and a closed padlock beside it. 3. Install automatic updates and turn firewalls on.

Good digital citizenship is about responsible and appropriate use of technology. Lessons should start early, but it’s never too late to adopt safer habits. Parents, in particular, struggle to keep up with kids’ digital lives, while also teaching kindness and digitally savvy. We encourage parents to talk to kids and use our resources.

A resume is no longer the only piece of information that can get you a foot-in-the-door. Your digital reputation can also play a critical role. Microsoft recommends: 1. Search your name online regularly. 2. Evaluate what’s there and correct inaccuracies. 3. Be mindful of your own digital footprint. 4. Cultivate a positive reputation.

2. How can Americans improve their digital citizenship?

Saylor Frase, CEO, Nuspire Networks

The main thing to use is skepticism. Just because it comes up in Google doesn’t mean you should click on it. Only shop on sites that have “https” with a yellow padlock in the address bar and keep your antivirus systems and firewalls, monitored and maintained properly.

Improve your internet literacy, which will allow you to avoid risks. Think about what you are posting: know that it is not yours anymore. You can’t take it back, it will never go away and the internet is not as anonymous as it seems; you are tied to that data forever.

Understand that your online identity is your identity. Most of the things posted on the internet are stamped with an IP address and/or GPS coordinates. Bearing this in mind, Americans should behave in the digital environment as if it were a busy street in New York City.

3. In our social media-friendly culture, how can we protect our digital identities?
Don’t let your business get sacked

Protect your team against targeted attacks

Any given Sunday...or Monday...or any other day of the week for that matter... cyber criminals are trying to break through your defenses. They’re crafting targeted attacks aimed specifically at your business to get around your existing security and steal your data.

Is your team ready?

We’re on your side. For the past 25 years, Trend Micro has focused on understanding and countering the latest cyber threats. We have over 1200 threat experts around the world, and help 48 of the top 50 companies protect their critical information every day.

Trend Micro Custom Defense is the only cyber security solution that enables the complete lifecycle needed to detect, analyze, adapt, and respond to targeted attacks.

Find out how Trend Micro can help defend your team against targeted attacks better than any other offering available today.

www.trendmicro.com/customdefense