Cyber Security

Kevin Mitnick: Inside the mind of the World's Most Famous Hacker.

Why your company's IT needs the cloud to keep pace **P4**

Experts share tips to steer you clear of threats **P10**

IN THIS ISSUE

Serve and Protect
ISA co-chairman Eric Cosman's overview of why securing the national infrastructure is challenging—yet essential. P8

Scam Free
AARP Fraud Network Ambassador Frank Abagnale breaks down the most worthwhile habits to put into practice to protect yourself. P12

READ MORE ON FUTUREOFBUSINESSANDTECH.COM

The Frontlines Online
An expert relays his account of cyberattacks today, as well as what's trending in security today and how companies can leverage it.

Silent Defenders: the Next Generation of Cyber Security

Continuing to safeguard the digital information and communications systems that are critical to our daily life depends on the next generation of cyber talent.

Renee Forney
Executive Director, Department of Homeland Security, CyberSkills Management Support Initiative

In every interaction I have with students, at all levels, they are surprised and intrigued by the cyber security work done by the Department of Homeland Security (DHS). As technology and threats change, we are constantly building a team to match. Today's students will be tomorrow's protectors of cyberspace.

Life with cyber

Cyberspace is a general term for our modern interdependent network of information and communications technology infrastructures, including the Internet. Today, cyberspace has become an integral part of life in America. Billions of computers and devices—ranging from mobile phones to the industrial controls used in power plants—provide enormous benefits to our society and economy.

The Nation now faces myriad cyber threats from criminals...

The Nation now faces myriad cyber threats from criminals, including individual hackers and organized criminal groups, as well as technologically advanced nation-states. Sophisticated attacks are the new norm, with even the most protected networks of the government and private sector experiencing intrusions. Attacks result in the loss of intellectual property, the compromise of personal data and potential threats to public safety.

New challenges daily

Everyday, leading cyber experts at the Department protect DHS technology and networks to ensure the effective execution of our many homeland security missions, including preventing terrorism, securing our borders and responding to natural disasters. Other DHS experts focus on specialized cyber security work in areas such as digital forensics, incident response, secure coding, cyber intelligence analysis and cybercrime investigation.

In future years, the number of opportunities at DHS—and outside of government—will continue to grow. I commend those students that are considering a career in the evolving field of cyber security, and I encourage educators and current cyber professionals to join us in promoting the cyber security opportunities available in both the public and private sectors. ■

Publisher: **Mac Harris** Business Developer: **Stephanie King** Managing Director: **Luciana Olson** Content & Production Manager: **Lauren Hubbard** Lead Designer: **Kathleen Edison** Designer: **Marie Coons** Copy Editor: **Sean Ryan** Advertising Manager: **Alana Giordano** Contributors: **Kristen Castillo, Eric Cosman, Renee Forney, Michael Kaiser, Diogo Monica, Jim Reavis** Send all inquiries to **editorial@mediaplanet.com** Cover Photo: **Dan Taylor/Heisenberg Media** All photos are credited to Getty Images unless otherwise credited. **This section was created by Mediaplanet and did not involve USA Today or its Editorial Departments.**

UNMANNED •

CYBER •

C4ISR •

LOGISTICS •

THE VALUE OF

LEVERAGING FULL-SPECTRUM CYBER TO NEUTRALIZE ENEMY THREATS.

Today, the world's most advanced weaponry is taking new form. Northrop Grumman's expertise in every aspect of cyber is transforming the global battlefield. From resiliency to agile defense, we're providing an increasingly effective advantage in combating evolving threats and challenges. *That's why we're a leader in full-spectrum cyber.*

***THE VALUE OF** PERFORMANCE.*

NORTHROP GRUMMAN

www.northropgrumman.com/**cyber**

NEWS

Up, Up and Away: Taking Traditional IT to The Cloud

Compared to the potential of cloud providers, sticking to the status quo when it comes to your business' IT will only get you so far—and that's not very.

The high profile breaches at the U.S. Office of Personnel Management (OPM), Target and Anthem were all attacks on legacy IT systems. If there is one thing these and numerous other security breaches making the news have taught us, it is that individual corporations and government agencies cannot protect their computers nearly as well as cloud providers, and they are only falling further behind.

Top-tier cloud providers and their ecosystem can make the investments in people and innovation to keep up with the hackers

Resource management

Top-tier cloud providers and their ecosystem can make the investments in people and innovation to keep up with the hackers, and provide businesses with professionally managed information technology.

Not only is cloud computing turning out to be a better model for IT, it is actually reinventing the information security industry by allowing organizations to purchase security capabilities on demand. We call this capability Security-as-a-Service, because it can not only help a corporation secure its headquarters but also extend the same security to branch offices, mobile devices and business partners that never traverse the headquarters.

This doesn't mean that cloud computing is immune to security breaches. No computer system devised is foolproof. However, the economics driving the cloud make it the only IT sector that can afford to adequately invest in security. Legacy IT is a sitting duck, no matter what compliance mandates we give to a business to improve its security. ■

By Jim Reavis, CEO, Cloud Security Alliance


Panic is no substitue for a plan.
Akamai
There's no hiding from hackers. If you're on the web, you're on their list.
Build a strong and confident defense against web attacks. www.akamai.com/dontpanic

INSPIRATION

Know Your Enemy: Tips from a Hacker

World-famous hacker-turned-security expert Kevin Mitnick shares best practices for staying safe in an increasingly exploited digital universe.

As far as Kevin Mitnick is concerned, there is a silent war happening around us all the time, wherever we may be. "But barely anyone knows it," the renowned computer security consultant adds. As a member of his own strategy team put it to him recently: "Those that do actually don't know at any given time who or why they are fighting."

In addition to being the CEO of his own Mitnick Security Consulting, Mitnick also works in partnership with KnowBe4, as their Chief Hacking Officer to provide the leading security awareness training available today. Checking in with Mediaplanet, he outlines the insider knowledge that makes him a living—and us safer.

What originally drew you into the world of hacking?

In high school, I met this other kid who could perform magic with the telephone. It was called "phone phreaking," and it facilitated my other great passion: pulling pranks. As the phone company started using computers to control devices, such as phone company switches, my interest in hacking began. When I started, it was completely legal and hacking was cool. Hackers were considered the whiz kids. My favorite hack of all-time, still to this day, was when I was young, hacking the McDonald's drive-through.

What are the biggest barriers a hacker faces when attempting to access private information?

Not much. Private information is freely available if you subscribe to the right databases, typically used by information brokers. These databases allow you to query a person's social security number, birthdate, current and past addresses, current and past phone numbers. Once this information is obtained, it's not too difficult to obtain the target's credit report online.

As far as gaining access to enterprise information, the biggest barrier is layered security controls. Meaning I would have to compromise several layers of security to break in. I travel the world and demonstrate live hacking at many conferences and speak to people of all walks of life. Lately, I've been showing how easy it is to steal someone's personal identity in about 60 seconds! By accessing some databases I'll know an individual's mother's maiden name, social security numbers—a whole bunch of stuff.

How does security for mobile devices differ from that of corporate services and PCs?

Most people don't even use security on their mobile phones, such as adding a passcode. The majority of people blindly use public WiFi in public spaces. If there is one thing anyone can take away after reading this is use a Virtual Private Network (VPN) service. One thing people should consider is purchasing a VPN subscription so that they can securely connect when using public Wifi. Basically, if you aren't using a VPN, your Internet traffic may be monitored, or worse, you may be hacked when using open wireless networks.

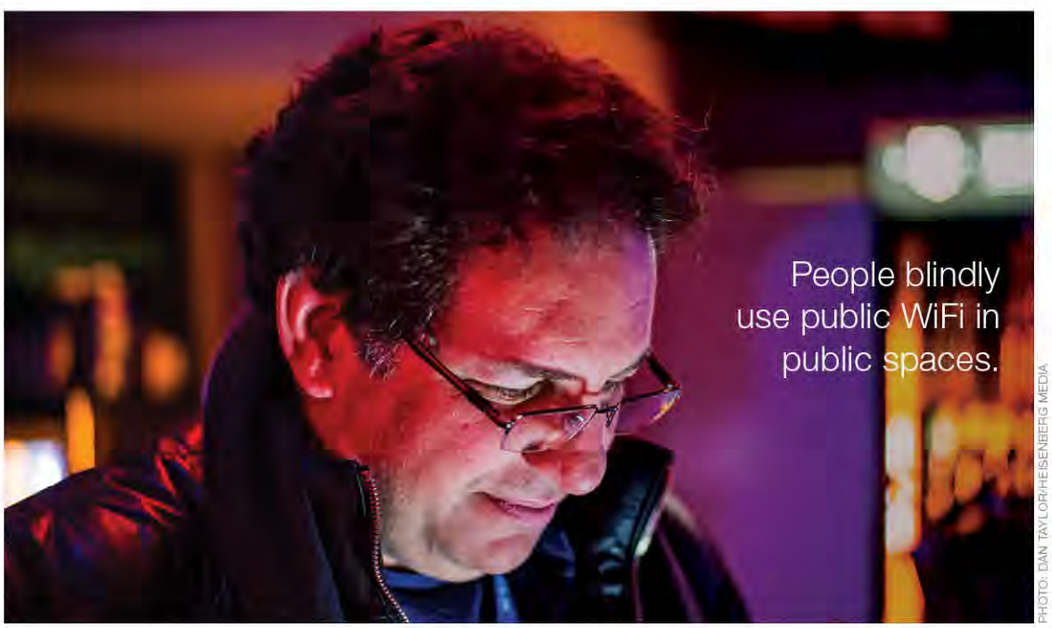


PHOTO: DAN TAYLOR/HEISENBERG MEDIA

What steps would you tell organizations to follow to improve their cyber security measures?

There are two important and easy steps that will provide much, much better cybersecurity for any organization.

Get tested regularly! Smart organizations are using the progressive strategy known as "red teaming." This is a rewarding practice of using external, independent teams to challenge organizations to find ways to improve their effectiveness. For cyber security this is known as Security Penetration Testing, the use of third-party penetration testers to simulate attacks by real intruders against systems, infrastructure and staff. The ultimate goal is to provide organizations with a thorough analysis of their current security.

Secondly, train all your Staff on what social engineering is and how to detect it. People are the weakest security link. They can be manipulated or influenced into unknowingly and innocently helping hackers break into their organization's computers and they can be manipulated into handing over the keys the kingdom. Social engineering is a technique used by hackers and con artists that leverages your tendency to trust. Providing security awareness training for staff is absolutely crucial in light of social engineering. ■

Read Kevin's full interview online at **futureofbusinessandtech.com**

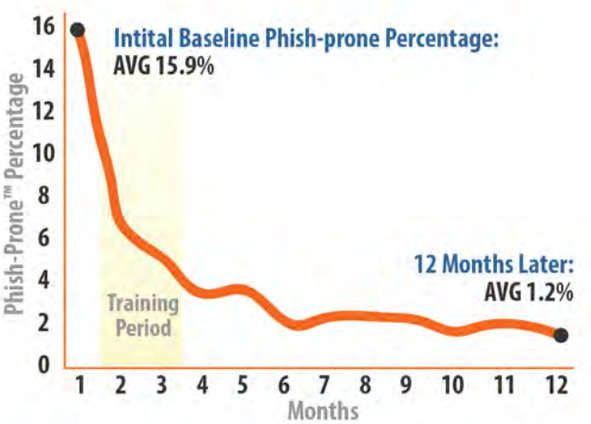
KEVIN MITNICK
Security Awareness Training

91% of successful data breaches started with a spear-phishing attack.

Cyber-attacks are rapidly getting more sophisticated. Based on Kevin Mitnick’s 30+ year unique first-hand hacking experience, you now can train employees to better **manage the urgent IT security problem of social engineering**.

1. Test your users with our **Free Simulated Phishing Test**
2. Train them with web-based interactive **Security Awareness Training**
3. Continue to send frequent **Simulated Phishing Tests**

Simulated Phishing Attacks



Get Started with Your FREE Phishing Test!

www.KnowBe4.com/FreePhishTest

KnowBe4, LLC | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: sales@KnowBe4.com

KnowBe4
Human error. Conquered.

INSIGHT

Detect, Respond, Recover: How to Keep Your Small Business Safe Online

Despite statistics to the contrary, many small businesses still believe they're not vulnerable to data breaches because of their size and limited assets.

Nearly half of small and midsized businesses (SMBs) have been the victim of a cyberattack, and 71 percent of security breaches target small businesses. The truth is, as larger companies beef up their defenses, those who wish to steal sensitive data are taking advantage of businesses that may lack the knowledge and the resources to keep their digital assets secure.

Grid for success

In 2013, the National Institute of Standards and Technology (NIST) established a "best practice" framework for reducing risks to the nation's critical infrastructure. This approach recommends five steps that any-sized company can take for addressing cyber threats:

1. Identify: Inventory your most valuable assets—the "crown jewels," such as employee, customer and payment data.
2. Protect: Assess what protective measures you need to have in place to be as defended as possible.
3. Detect: Have systems in place that would alert you if an incident occurs including the ability for employees to report problems.
4. Respond: Make and practice an incidence response plan to contain an attack and maintain business operations in the short term.
5. Recover: Know what to do to return to normal business operations after an incident or breach, including assessing any legal obligations.

Daily improvement

Businesses can improve their online safety practices every day by following these tips:

- Keep a Clean Machine: Having the latest security software, web browser and operating system in your business are the best defenses against viruses, malware and other online threats.
- Protect Information: Secure accounts by adding two-factor authentication and making passwords long, strong and unique.
- Protect the Company's Online Reputation: Set security and privacy settings to your comfort level of sharing.
- Educate Employees: Teach your employees basic best practices. For example, if an email, social network post or text message looks suspicious—even if you know the source—delete it.

By Michael Kaiser, Executive Director, National Cyber Security Alliance

Where Cyber Security Serves National Interest

Whether it is the purification of our water, the preparation of our food or the generation of electricity, automation ensures safe and reliable operation of a wide variety of industrial processes.

Digital security applies to virtually all applications of computers and communications, some of which the public may not even be aware of—like monitoring and controlling various elements of the national critical infrastructure. Attack, compromise or failure of these processes can have dire consequences for society, ranging from loss of vital services to major environmental damage or even loss of life.

Staying strong

Ensuring this protection involves the application of proven standards and practices, such as those offered by the International Society for Automation (ISA). As a global, unbiased developer of technical resources focused on process safety and control systems cyber security, ISA brings a unique perspective and deep understanding of today's industrial challenges.

This understanding is reflected in the ISA/IEC 62443 standards that define requirements and procedures for implementing electronically secure manufacturing and control systems and security practices, and assessing electronic security performance. These standards, and the associated training, certification and certificate programs, cover the complete lifecycle of cyber security protection.

Putting plans in motion

ISA and the Automation Federation helped to prepare the U.S. Cyber Security Framework—released in early 2014—and helped to implement the provisions of the U.S. Cyber Security Enhancement Act.

Manufacturing and operating companies in a wide variety of industries are working with suppliers and engineers to apply these standards in combination with specialized skills and proven practices to develop and implement cyber security management systems to protect our national infrastructure—and our way of life. ■

By Eric C. Cosman, Co-Chairman, ISA/IEC ISA/IEC 62443; Principal Consultant, Standards Committee, OIT Concepts

INDUSTRY PERSPECTIVE

Life Hack: Staying Ahead of Cyber Threats

We polled a trio of industry experts to better understand what identity thieves are looking for, and how you can outpace them to keep your privacy protected.

Bill Stewart
Executive Vice President,
Booz Allen Hamilton

What are some tips that we can use to improve our security online?

When you pick passwords and PINs, go long and use a password manager to pick unique passwords—especially for email and bank sites. Then, stay aware. When you are shopping or providing information online, look for the green lock symbol and "https" in the address bar indicating that the site has strong security protections. You can also click on the lock to see more security information about the site.

In the future, how do you think cyber security will combat privacy threats?

Moving forward, cyber security will take a two-pronged approach to manage these risks: Predictive intelligence and advanced security systems. Predictive intelligence will minimize initial attacks and prevent the same attack on multiple companies. Advanced security systems will focus on protecting the most sensitive information using encryption and other tools.

How can we protect our digital identities in the age of social media?

Most social media sites make money from advertising, so the more they know about you and your friends, the more valuable their ads can be. You can change privacy and security settings on each site to limit who can see what you post and how much they can see. Once you post it online, it can be nearly impossible to remove from the Internet.

Dan Shugrue
Director, Security
Product Marketing,
Akamai Technologies

Use different passwords for different websites, and change them often. If you have trouble keeping track, use a password manager application that allows you to use the web the way you normally use it. If you access from several devices, make sure you buy an app that allows you to access passwords from different devices.

Web security has evolved from a "perimeter-based" to a "defense-in-depth" approach. As more applications and sites move to the cloud in order to save money, share data and generally become more agile, so will security. Organizations and individuals will have to carefully weigh the costs and benefits of doing business on and getting their security from the cloud.

The bigger social media platforms are making it easier to control which groups of acquaintances, friends or family see which of our posts. If we are aware and conscious that what "goes up" in the social media age does not necessarily come down, we can be smarter about what we post in the first place. And only accept friend requests from people you've actually met.

Davis Hake
Director,
Cybersecurity Strategy,
Palo Alto Networks

The best action individuals can take to strengthen digital security is to enable two-factor authentication. After entering a password, you receive an SMS with a code that is then required to log on. However, recognize that sensitive personal information shared online will be as secure as the organization holding it.

It is cheaper than ever to launch more attacks of greater sophistication, and consequently more expensive and difficult than ever to detect and respond to them. The future of cyber security, therefore, lies in integrated platforms of technologies designed to automatically communicate and collaborate that prevent attacks across their entire lifecycle.

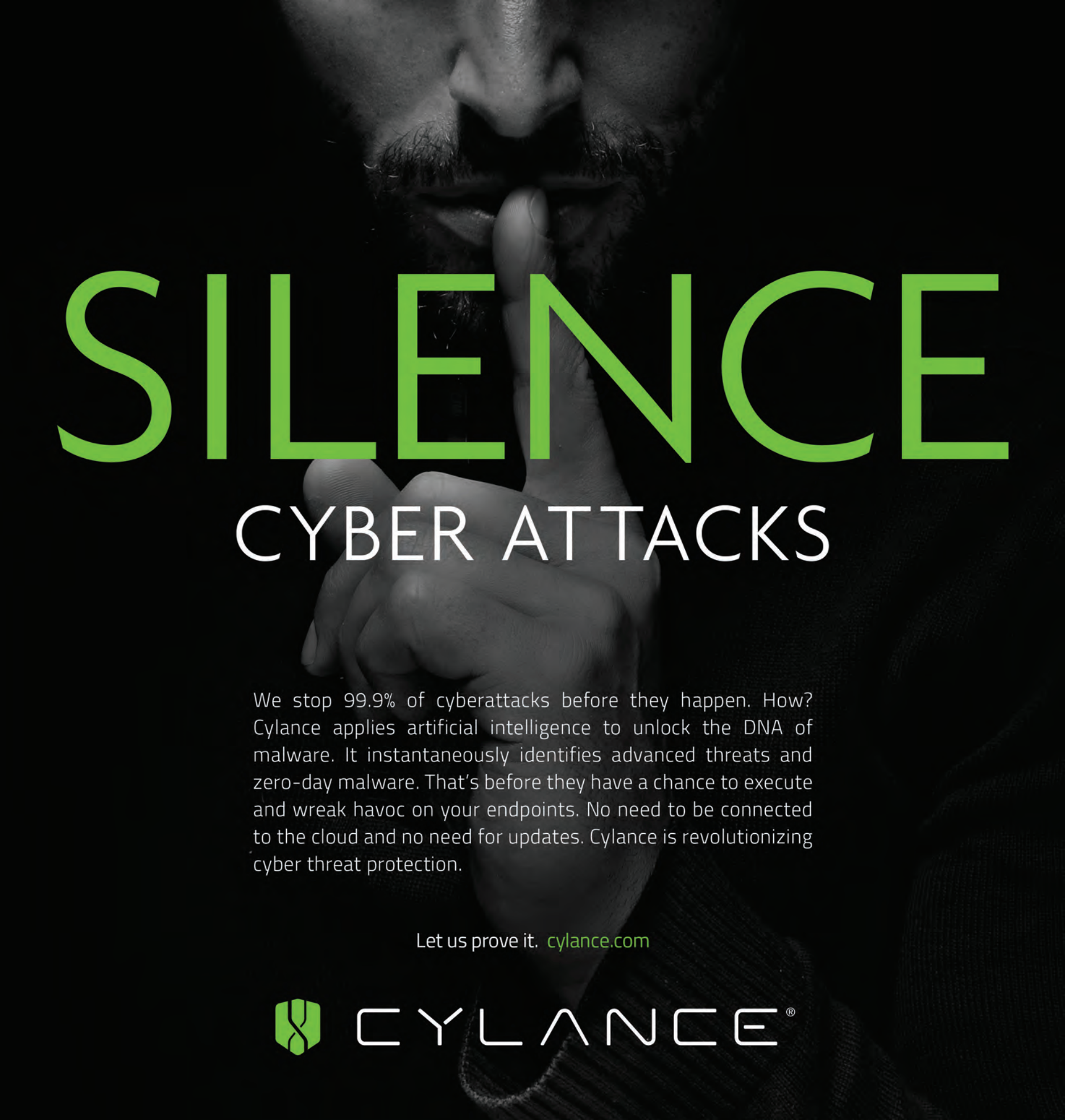
Social media has become an incredible way of keeping in touch. However, attackers also use these outlets for reconnaissance on targets—use information about your family members, job and hobbies to craft detailed spearphisihing e- mails allowing them to hijack your computer and threatening the security of your personal data or your company.

Stuart McClure
CEO/President
and Founder,
Cylance

Start off by assuming that you are a target because, in truth, we all are. Take caution on how much personal information you put on Facebook, LinkedIn and other social media sites. Hackers troll those places for information. Be wary of that email with a plausible but still unusual request—even if it's from a person or a business you know.

New approaches using highly advanced artificial intelligence, algorithmic science and machine learning are starting to be widely deployed in businesses worldwide, and stopping attacks before they have a chance to execute. The application of advanced computer technologies to cyber security will form the foundation of future defenses.

Start by recognizing that it's not just your digital identity, but your entire identity, and that the information you promote through social media networks is accessible to everyone, everywhere. Recognize the potential risks of publicly disclosing personal details in such a public forum... and who you befriend online.


SILENCE
CYBER ATTACKS
We stop 99.9% of cyberattacks before they happen. How? Cylance applies artificial intelligence to unlock the DNA of malware. It instantaneously identifies advanced threats and zero-day malware. That's before they have a chance to execute and wreak havoc on your endpoints. No need to be connected to the cloud and no need for updates. Cylance is revolutionizing cyber threat protection.
Let us prove it. cylance.com
CYLANCE®

ADVOCACY

Your Fare Share: How to Protect Your Identity Today

FRANK ABAGNALE AND ASSOCIATES

Frank Abagnale, the Fraud Watch Network Ambassador for AARP, opens up about identity theft—and suggests everyone use more caution before doing the same.

Many Americans first learned about him through the portrayal of his life story in the film "Catch Me If You Can." But for the last few decades, Frank Abagnale has helped Americans by helping to nab the type of criminal he once was. Today, he faces the challenge of educating others, particularly senior citizens, about the threats surrounding them today.

How has modern technology affected the likelihood of identity theft?

Identity theft has actually been around since the 1970s, before the Internet, e-mails and data storage. In the old days, this crime was committed by very few because it took a great deal of research and legwork. For example, they would read in the newspaper that Bob Smith was named Homebuilder of the Year. As they read the article, they picked up that Mr. Smith had filed for bankruptcy ten years earlier but has now worked his company out of the bankruptcy and is one of the wealthiest and most successful builders in the country.

The identity thief would take a walk to the bankruptcy court and make a copy of the microfiche of the bankruptcy filing. The identity thief would then use this public record to capture Mr. Smith's full name, his wife's name, his date of birth, her date of birth, his social security number and her social security number and then stole their identities. Today, due to technology, an identity thief can do the same thing from as far away as Moscow in their pajamas sitting in their kitchen with a laptop.

What would you say are the most important habits for protecting your identity today?

First, shred any documents that contain personal information that you no longer need. Use a micro-cut shredder. This is a shredder that turns paper into pieces the size of rice and cannot be put back together like straight and criss-cross shredders. Second, use a credit monitoring service that monitors all three credit bureaus and notifies you in real time. Third, only use a credit card—not a debit card. This way, if someone was to steal your information and charge $1 million dollars on your credit card, your liability is zero. They are only accessing the credit card company's money, not yours. When you pay the bill every month, your credit score goes up. When you use a debit card, you do nothing for your credit score. It is my personal belief that the credit card is the safest form of payment on the face of the earth.

Be careful when writing checks. If you leave a check at a retail store, on that check is your name, address and phone number, your bank's name and address, your account number at that bank, your routing number into that account (wiring instructions), your signature on the signature card at the bank and then the clerk has written your state drivers license number and your date of birth on the front of the check. We live in truncation, which means you do not get the physical check back. Anyone who sees that check has more than enough information to become you, wire money out of your account or order checks with your account information that would be written and debited against your account.

> If you use Facebook, never state your date of birth and where you were born...

Social media—if you use Facebook, never state your date of birth and where you were born on your Facebook page. Otherwise you might as well say, "Come steal my identity."

How do the risks to seniors differ from those facing younger generations?

Unfortunately, many seniors live alone and when people contact them by phone and the Internet and pretend to befriend them, they can easily fall prey to their scams. The most common scams we see against the elderly are sweepstakes scams.

For example: You won a new Mercedes but you will have to send us a fee or tax before we reward you the gift. You receive a phone call from someone who says they are with the IRS and you owe back taxes. If you don't pay them in 24 hours, they will put a lien on your property. You receive an email that appears to come from Microsoft claiming there is malware in your computer and they need to have access to your computer to remove it. They then steal all of the data on your computer, family pictures, banking information, etc. and then tell you that if you don't pay a ransom you will never get it back.

The truth is, even if you paid the ransom, you are never going to get the files back. Always remember, no bank or government agency is going to call you and ask you for your social security number or personal information. Just hang up the phone. ■


Every
2 seconds
someone's
identity
is stolen.
We're fighting back with the **AARP Fraud Watch Network**. It provides resources to help you spot and avoid identity theft and fraud so you can protect yourself and your family. And it's free – even if you're not an AARP member. **To learn more about how you can protect yourself and your family from fraud visit AARP.org/FraudWatchNetwork**
FRAUD WATCH NETWORK
AARP Real Possibilities

ASK THE EXPERT

Job Alert: Cyber Security Preps Kids for Many Careers

By Kristen Castillo

High tech gadgets are a major part of kids lives and the world around them. At the same time, crime, fraud and scams are lurking online.

Kids need to develop cyber skills and transition those skills into a rewarding career, or so says Christopher Valentino, the strategy director of the Cyber Division for Northrup Grumman Information Systems. As a father of three, Valentino sees firsthand how kids use technology. He checks in with us to share what he's seen so far and expects moving forward.

When is it a good age to teach kids about cyber studies?

Pre-kindergarten is the best way to start. The way kids are exposed to technology at such an early age. As they learn to read and write, then they have cyber free will. They interact with the device much differently when they understand I put an input in and I get something out.

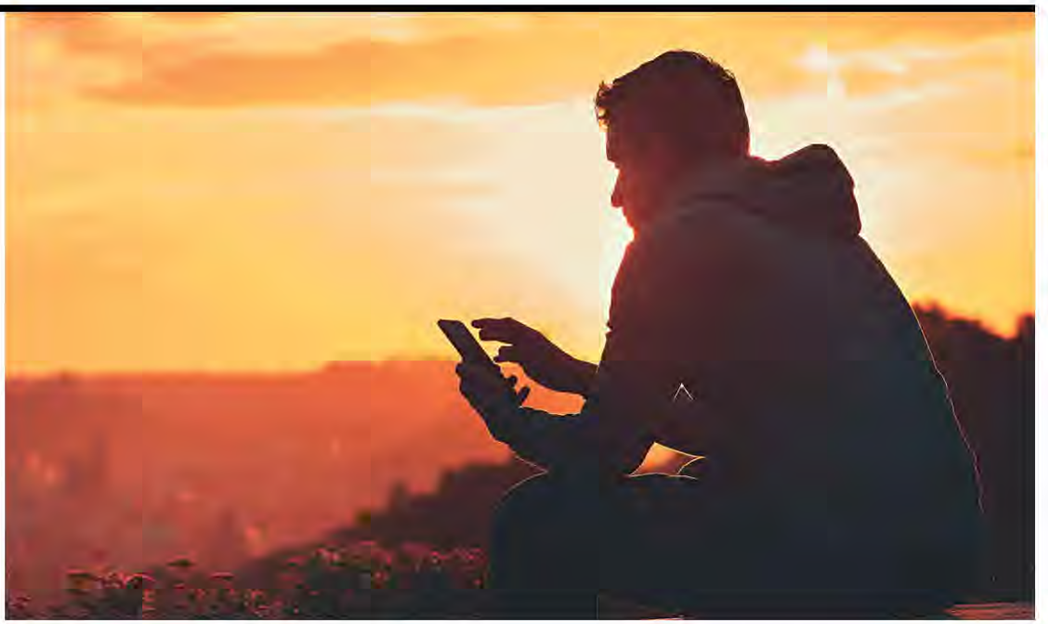
By 2017 there will be a shortage of 2 million cyber security jobs. Why is there such a growing demand for cyber security careers?

All the recent breaches and attacks—people are really aware. It becomes very personal when people take your information and redistribute it to nefarious people on the Internet. Because of the awareness and the state of the problem, it's generated demand beyond what the current system can supply.

Can you explain the benefits of pursuing a career in cyber security?

It's very rich for innovation at all levels. There's incredible flexibility. The skills are very portable. You became very marketable across a very broad range of business sectors. Whenever you're in an economic situation where people want you, people need you, there's certainly opportunity for good compensation.

Learn more about careers in cyber security at **futureofbusinessandtech.com**



Guarding Against the Internet of "Crappy" Things

Some claimed 2015 would be the year of the Internet of Things (IoT), yet it has quickly turned into a year of mostly negative press.

Security in regards to the Internet of Things is a very hot topic. Much of the coverage so far has centered on the vulnerabilities of first-generation IoT devices, leading to unflattering media attention dubbing this as the "Internet of Crappy Things."

In focus

There are a few characteristics that make these IoT devices particularly hard to protect:

- The majority of these devices are made to be cheap and have very limited interfaces (no keyboards or displays).
- There is the need for ease of use and installation, which usually leads to insecure defaults out of the box.
- Resource constraints such as lower battery power and CPU speeds make it hard to use the latest security protocols.

These characteristics, together with the sheer number of distinct use cases for these devices, make it incredibly difficult to standardize on a single platform and get a consensus on how to implement security mechanisms.

Looking ahead

The good news is that these problems are being raised a lot earlier than they have been in other technologies. The sensationalizing of security issues found in internet-enabled cars, thermostats and fridges is indeed pushing manufacturers to take these issues more seriously.

A good example of a company raising the bar for the security of IoT devices is Apple. By adding strict security requirements on their Homekit certification, they have effectively raised the bar for security and ultimately made their customers safer.

Unfortunately, maturity in the IoT field is still at least five years away. In the rush to bring new products and services to market, many companies will overlook basic security considerations such as secure software updates, authentication and access control. Until then, I'm afraid we are indeed stuck in the Internet of Crappy Things. ■

By Diogo Monica, Member, IEEE; Security Lead, Docker

GOING BEYOND SECURITY

Cyber security today is nonnegotiable. As our world becomes increasingly connected, the threats to your business also increase. But the future of cyber goes beyond IT and compliance. Cyber done well should secure your organization to streamline operations, build trust with customers, boost your reputation, and benefit the bottom line. At Booz Allen Hamilton, we partner with companies to develop and manage cyber programs that create competitive advantage through the right mix of people, processes, and technology. Our intelligence-driven approach blends strategic insights with innovative technologies that help your business thrive. To learn more, visit **www.boozallen.com/cyber-solutions**.

*We are currently hiring for cyber security analysts, cyber incident handlers, and more. Visit **www.boozallen.com/careers** for a complete list of related positions.*

Booz | Allen | Hamilton

SUCCESS IS BLACK AND WHITE.

THERE'S NO GRAY AREA WHEN IT COMES TO YOUR CUSTOMERS.

You either have what they're looking for, or you don't. And behind every item they see is a work order that helped it get there. Every time. On time. The Canon MAXIFY lineup of printers was built to keep those orders flowing:

- LOW COST PER PRINT
- QUICK FIRST PRINT
- MOBILE DEVICE PRINTING
- CLOUD CONNECTIVITY
- 100% US-BASED SERVICE & SUPPORT

Because this is your business. Keeping your shelves filled with the right products is on you. That makes what comes out of your printer more than just paper and ink. It's the way your business moves into the black.

YOURS TO MAKE

MAXIFY | Canon SEE IMPOSSIBLE

USA.CANON.COM/MAXIFY