Colleagues,

As I write this we are preparing for our annual Cyber-security Training Forum with over 500 attendees... WOW, what a great response and I'm optimistic the conference will be well received. As an organization we have worked very hard to find speakers to speak on subjects that are very important to us all. A special thanks to Mr. Glenn York for his work in helping to recruit some outstanding speakers that we haven't had speak at our conferences in recent years, or in some cases ever. Thanks Glenn for stepping up and making a difference!

So, what's next for the chapter? During the next 5 months we will continue to have regular membership lunch and dinner meetings, we are planning a fall conference to be held at the University of Colorado in Colorado Springs (UCCS), we have our recognition luncheon in December, and intermingled with everything will be a continued emphasis on growing our membership. While we're excited to host the conference next week, things won't stop when that is over. As a reminder, because we are hosting a conference in August there will not be regular membership meetings in August. These will start up again in September.

I recently saw the e-mail from ISSA International announcing annual award winners for ISSA and noted that we weren't represented on that list. I made a decision earlier this year that our chapter would be better postured to compete next year, based on events occurring this year, so I am keeping a list of "things" our chapter is doing this year that we can submit a winning package in 2015. In addition, I'll send out some specific criteria over the next couple months for the individual

(Continued on page 3)
How elite hackers (almost) stole the NASDAQ

By Dan Goodin, ArsTechnica, July 17, 2014

In 2010, elite hackers, most likely from Russia, used at least two zero-day vulnerabilities to penetrate the computer network operated by Nasdaq Stock Market, a hack that allowed them to roam unmolested for months and plant destructive malware designed to cause disruptions, according to a media report published Thursday.

The intrusion initially caught the attention of officials inside the National Security Agency, the Central Intelligence Agency, and departments of Defense, Treasury, and Homeland Security for two reasons, Bloomberg Businessweek journalist Michael Riley reported in an article headlined How Russian Hackers Stole the Nasdaq. One, it appeared to be the work of hackers sponsored by Russia or another powerful nation-state. Two, far from the typical espionage campaigns that merely siphon out secret data, the malware involved in the attack contained what early on appeared to be a digital bomb that could cause serious damage.

Riley’s 3,100-word cover article traces the resulting federal investigation, which also involved the FBI, Secret Service, the National Cybersecurity and Communications Integration Center, and on at least three occasions, briefings provided to President Barack Obama. Ultimately, analysis of the malware showed its capabilities were less destructive than earlier believed, but there was still cause for concern. As Ars reported last year, it came around the same time that five eastern European men allegedly breached networks belonging to Nasdaq and at least seven other financial institutions. According to federal prosecutors, one of the suspects, upon gaining persistent control over the world’s second biggest stock exchange, proclaimed "NASDAQ is owned."

"While the hack was successfully disrupted, it revealed how vulnerable financial exchanges—as well as banks, chemical refineries, water plants, and electric utilities—are to digital assault," Riley wrote of the 2010 campaign. "One official who experienced the event firsthand says he thought the attack would change everything, that it would force the US to get serious about preparing for a new era of conflict by computer. He was wrong."

The article continued:

What the investigators found inside Nasdaq shocked them, according to both law enforcement officials and private contractors hired by the company to aid in the investigation. Agents found the tracks of several different groups operating freely, some of which may have been in the exchange’s networks for years, including criminal hackers and Chinese cyberspies. Basic records of the daily activity occurring on the company’s servers, which would have helped investigators trace the hackers’ movements, were almost nonexistent. Investigators also discovered that the website run by One Liberty Plaza’s building management company had been laced with a Russian-made exploit kit known as Blackhole, infecting tenants who visited the page to pay bills or do other maintenance.

What one investigator referred to as "the dirty swamp" of Nasdaq’s computer banks made following the trail of the Russian malware excruciatingly slow. The agents figured the hackers first broke into Nasdaq’s computers at least three months before they were detected, but that was just a guess. There were indications that a large cache of data was stolen, though proof was scarce, and it was hard to see what was spirited out. "If someone breaks into your house, trying to figure where they went and what they took is pretty difficult because, unlike a bank, you don’t have cameras in your house, you don’t have motion sensors," says Jason Syversen, chief executive officer of Siege Technologies, a security firm in Manchester, N.H. "In terms of cybersecurity, most companies are more like a house than a bank."

Read the rest here:

Welcome!

First, I’d like to welcome those new members on behalf of the Chapter! When you’re participating in Chapter activities, please take a moment to introduce yourself to members of the board, me, and other members. Don’t forget to identify yourself as a new member and feel free to ask for help or information.

Thanks for joining the Chapter and don’t forget to look for opportunities to lend your expertise to improve the Chapter. We’re always open to new ideas and suggestions.

We will continue to sponsor student memberships so if you are interested, please contact me to coordinate the details. Each membership costs $55 per year including chapter dues. I’ll be happy to work with you if you have special requests such as male/female, veteran, etc. Contact me if you’re interested in becoming a sponsor. Also, if you know a specific student at any of the local universities you’d like to sponsor, I can work with you on that too.

We have good news about our 2014 membership drive so far. We’ve added 9 new members so far in the third quarter of the year for a total of 67 new members this year. So, everyone, give yourself a pat on the back and continue to bring in new members. We still need at least another 20+ new members to hit our recruiting goal for the year. Also, don’t forget to remind your peers and friends to renew, too. We’ve still got some work to do to get to our goal of 400 members.

As a separate activity, we are establishing a student mentorship program. Melissa Absher is the chairperson of the Student Mentorship Committee. The student membership mentoring program now has a solid base of mentors, but is looking for more. Thank you to all who have volunteered already. Please see Dave or Melissa if you are interested.

Thanks for all your efforts and support.

David Reed
Membership Committee Chairman
dreed54321@comcast.net

A Note From Our President

awards and if you are making a positive difference within the cybersecurity community that the board may not be aware of I would ask that you make us aware of it so we can recognize you for your efforts. We also need to recognize members of our chapter for lifetime achievements as we have several members who have helped mold this career field at very high levels. I know that our chapter is full of difference makers, and we need to, and will, highlight those efforts.

Hope to see everyone at the conference and look forward to watching our chapter continue to do great things the rest of this year. As always, if you have suggestions or comments please call me at (719) 360-4543 or e-mail me at plaverty1961@gmail.com. Thanks!

Pat
US and UK Consumers Avoid Pirated Content

Illegally obtaining TV and movies is almost endemic in the Asia-Pacific region though.

By InfoSecurity, July 11, 2014

Pirated TV an film content is risky for consumers from a cybersecurity perspective and takes millions out of the creative and media economy on an annual basis. But the counterintuitive good news is that the majority of US (70 percent) and UK consumers (72 percent) are unlikely to watch ill-gotten entertainment, at least according to survey responses.

According to a global consumer survey from Irdeto, more than 90% of those in the US and 52% in those in the UK who do watch pirated content say it is a few times a year or less, signaling that in markets where more content is available, there is less of a need to download it illegally.

Overall, globally, while viewing of pirated content is clearly prevalent, many consumers would prefer to access content through legal channels. In fact, in areas where piracy is more common (Australia, where 26% admit to piracy, and Singapore, where 31% do) the main reason was because the video content is not available legally in their location.

Also, price was a top driver for consumers in India (29%) and Indonesia (36%) to watch pirated video content.

The portion of respondents who noted they were unlikely or extremely unlikely to watch pirated content was 40% in Australia, 31% in Singapore, 40% in India and just 9% in Indonesia, leaving a large majority of consumers in Asia-Pacific who are open to consuming entertainment through illegal means.

“One of the most interesting findings from our survey was that availability, poor quality and security issues are deterrents for downloading illegal content,” said Bengt Jonsson, vice president of APAC at Irdeto, in a statement. “This is a clear message to operators to provide high quality content at the right price. This could be a differentiator to remain competitive in a diverse region like Asia-Pac.”

Conversely, 62% of 18 to 24 year olds in the UK and 54% of 18 to 34 year olds in the US admitted to watching pirated content, a number much higher than older respondents. This highlights that young people are more willing to embrace piracy to get what they want.

Read the rest here:
http://www.net-security.org/secworld.php?id=16981
RPI Group
IA2

RPI Group Training in conjunction with authorized trainer, IA2, is offering National Security System (NSS) Accredited 4012 & 4015 Training hosted by SERCO at 1050 N Newport Rd, Colorado Springs, CO 80916

September 15-19, 2014

This course provides Five Days of interactive, highly concentrated, non-technical professional training necessary to achieve the in-depth knowledge, skills, and abilities needed to enforce Information Assurance (IA) requirements, apply Information System Security (INFOSEC) methodologies and facilitate certification and accreditation (C&A) activities by Fully Qualified Certification Agents.

All Training Materials & Exam included!

Training Seat Price $1495.00 per student.

For more information contact info@RPiGroupInc.com
ISSA-COS
July Financial Report

Income:

$675.00  Jun Membership Dues
$800.00  Award from Salient
$0.01  Jun Savings Dividend
$0.46  Jun Checking Account Dividend

$1,475.47

Expenses:

$847.88  TREA Lunch, Jun
$10.00  Tip Lunch
$452.14  TREA Dinner, Jun
$10.00  Tip Dinner
$110.00  Reimbursement for two student memberships
$110.00  Reimbursement for two student memberships
$120.00  Chapter sponsored retired membership
$120.00  Chapter sponsored retired membership

$1,780.02

Projected Expenses:

$110.00  Membership, reimbursement
$10.00  Lunch Tip reimbursement
$10.00  Dinner Tip reimbursement
$130.00

Account status:

Savings  63.37
Checking (#10)  10885.37
Membership checking  1434.87
Travel Support checking  100.00
Training checking  93.25
Cash (change/tips)  0.00
PayPal Account  985.23

TOTAL  13,562.09
Request for Chapter Presenters

We are over half way through the year and only had one sponsor so far. We will continue to talk to potential sponsors however due to tighten budgets, they have not been available. As such we are looking for members to present at both the lunch and dinner meeting. The presenter has about 40 minutes to give the presentation and answer questions. This could be one slide with a situation identified and audience will then discuss possible solutions or a how to presentation with a demonstration afterwards. The below listed are topics that have been suggested as areas of interest from our members. Please send an email to either, Pat Laverty (plaverty1961@gmail.com) and/or myself, Cindy Thornburg (thornbuc@aol.com) with topic to be presented, and we will connect with you for your availability. We would like the topic to be presented at both meetings however we do understand that may be difficult to accomplish.

- Cyber Security Laws in Colorado
- Interior Protection
- Building in Resiliency
- Ethics
- Intrusion Detection/Prevention Systems – configuration and how to review
- Making the Business Case for Security – how to
- Hacking – how to
- Application Security Scanning
- COMPTIA CE Cycles & Fee Structure
- A Summary and Rating of available Certifications
- A Survey of current IA Incidents We Should Know About (heartbleed) and What They Mean for the State of Our Industry
- Latest Innovations in Network Management Systems
- Real World Case Studies
- Threat Overview – Real World
- Legal Issues in Information Systems
- Asymmetric Warfare – what is it
- Spear Fishing – what is it and demonstration
- Prevention of Cyber Bullying
- Best Practices for Backing Up & Archiving Corporate Data
- When to Maximize or Minimize Your Cyber Footprint/Persona
- Threat Structuring
- Security Modeling – how to
- Data Flow Control
- Trusted Software Development – how to
- Risk Management Framework and what does it mean
- Case Study of Breaches – how they happen and how to prevent
- Security Architecture Development – ‘Building it In’
- ‘Mobile’ Security Management
- Bring Your Own Device (BYOD)
- Biometric Security and Privacy
- Hacking Back

Thank you!

Cindy
Russian government offers money for Tor-cracking tech

By Help-Net Security, July 28, 2014

The release of the Risk Management Framework (RMF) methodology in March 2014 may have caught some in the DoD community flat-footed. For many others, the response by those on their toes and immersed in cybersecurity the attitude has been, "It's about time".

The Russian Ministry of Internal Affairs (MVD) has published a tender offering $111,000 to any Russian company or organization that can provide technology that can de-anonymize users of the Tor anonymity network and decrypt the data sent through it.

The tender, which was published earlier this month, was recently changed to say that the offered money was for research work on the Tor cipher.

"The competition is arranged by the Russian Government 'in order to ensure the country’s defense and security',' noted cyber security expert Pierluigi Paganini, a member of the ENISA's Threat Landscape Stakeholder Group.

"I asked a colleague to help me to translate the original tender [...] The tender is about the Tor indeed. The term 'Scientific Production Association' is a Soviet/Russian cover word for a military or a KGB/FSB R&D outlet. The one in question belongs to the Interior Ministry which is in charge of police and penitentiary."

In order to participate in the "competition," companies have to be based in Russia, have high level security clearance, and have to pay a fee of about $5,555 to get their solutions considered. They have until August 13 to send in their offers.

Originally sponsored by the US Naval Research Laboratory, the development of Tor is still partially backed by the US Department of Defense and other US government agencies.

It's used across the globe by journalists, political activists and dissidents, users concerned about their privacy, and criminals - anyone who is interested in hiding their identity and that of their contacts on the Internet, and circumventing national censorship efforts. It's also used by NSA whistleblower Edward Snowden.

Tor is used widely in Russia and, earlier this year, a non-specified Russian entity has been spotted eavesdropping nodes at the edge of the Tor network.

Read the rest here:
http://www.net-security.org/secworld.php?id=17174

8 online safety rules for college-bound kids

By Help-Net Security, July 22, 2014

Iovation is providing eight digital safety tips for college-bound kids. Previous generations didn't need to have "the digital talk" but in a world where what goes online stays online, it's essential.

1. The Internet is forever - Think about future employers, including those coveted summer internships. Don’t post anything online, including inappropriate photos, which would make a future employer think twice about hiring you. Good judgment is something employers look for, show that you have it.

2. Don’t add your address to your Facebook profile - Keep your address private. Anyone who needs your address can get it from you directly.

3. Don't broadcast your location - Go ahead and check-in at your favorite coffee place and post photos of you and friends at a concert. Just do it sparingly. People don’t need to know where you are all the time or when your dorm room or apartment might be empty.

4. Don't "friend" people you don't know - Be choosy when it comes to friending people on social media. Just because someone sends you a friend request doesn’t mean you have to accept it—especially if you have no idea who they are.

5. Guard your social security number - Your social security number is a winning lottery ticket to a fraudster. It is the key to stealing your identity and taking over your accounts. Keep your social security card locked away in a safe place. Memorize the number so you can minimize using the card itself. Question anyone who asks for your social security card. Employers, banks, credit card companies and the department of motor vehicles are some of the few legitimate entities who may need your social security number. Never give it out online or in email.

Read the rest here:
http://www.net-security.org/secworld.php?id=17150
Skeletons in Your Client's "Digital Closet"

*Due to the quick loss of potentially valuable facts in human memory, we must sometimes tap into digital devices to retrieve critical case information.*

By Martin Siefert, DFI News, June 4, 2014

Legal proceedings often rely on human memory for events and the sequence of those events. Studies have shown that individuals are notoriously bad at remembering details about past events. Without replenishing or review of perceptions, neural traces in the brain degrade and information is lost. Digital forensic investigations have played a pivotal role in many highly publicized cases and those same forensic techniques can be applied to recreate seemingly routine events that humans typically forget. This article will examine how the use of digital forensics can aid the legal profession with fact finding to support or refute eye witness testimony involving details of events.

The decay curve that models the human mind related to the amount of forgotten facts is initially a very steep logarithmic function and shows how many natural processes, such as radiation, diminish with time; it is ubiquitous throughout science.

Digital devices, however, are very good at "remembering" such otherwise forgotten details. A modern analysis of digital devices is commonly overlooked as a source of important and case-changing information. Because of the quick loss of potentially valuable facts, attorneys, law enforcement, and investigators must sometimes use a forensic digital examiner to tap into digital devices and retrieve critical information. Digital forensic capability is explored herein after the human memory ability is briefly reviewed and modeled.

**The Basic Hypotheses**

Psychologists have approached the subject of forgetting in various ways. Psychologist Donald O. Hebb first applied a decay curve formula to memory loss. Memories certainly fade over time, but how quickly the details about past events fade differ from individual to individual. Several studies support this rapid-loss-of-information model. Among many hypotheses, two fundamental representations exist to determine the decline in recollection of events. The first considers that there is no correlation between the amount of information or number (N) of facts learned and the time frame (t) over which it is forgotten. According to the first model, it does not matter if someone is given 10 or 20 items/facts (N) to remember—the rate by which it is forgotten remains constant.

The second hypothesis asserts that the amount of original information learned does indeed have an effect on how quickly information is forgotten over time. In the example above, the 20-item learning set typically, yet counterintuitively, results in a longer memory retention period than the 10-item set. In this article, the second hypothesis is accepted and used.

As Figure 1 shows, the loss of information happens exponentially from the time an event occurs. In this example the item set (N) of 20 and a delay of three days (t) is assumed. The result is a loss of 77.7% of facts (P) since the time an event occurred three days prior. What is especially interesting is that there is a significant memory loss happening within the first five to six days. How does this relate to an investigation or legal matter? Consider for a moment the time that transpires before a client seeks counsel or initiates a conversation about an event. Taking such delays into account, it is obvious that crucial information might be missed when relying only on human memory. Furthermore, studies have shown that eyewitness accounts are extremely unreliable and sometimes even produce misleading information. The combination of rapid decline of details in memory and unreliable eyewitness reports seems to make it incredibly difficult to obtain factual data.

**The Digital Device Model**

As mentioned earlier, digital devices such as computers, tablets, and cell phones are very good at "remembering" past events and should be used more often for such purposes. Using the same decay formula as in Figure 1, Figure 2 shows a hypothetical scenario of events that digital devices may have recorded, yet are overlooked by a client or fact-finder.

In only three days, a series of events took place that a person may have already forgotten, yet are conveniently stored on digital devices. Although this example reflects a small number of events (20), it can be assumed that over a period of three days a significantly larger number of data points were recorded. One other consideration might be that various applications on mobile devices record GPS (global positioning system) locations as the device is being used. Such activity may happen without the user’s knowledge. This process of "geo-tagging" information is briefly touched on later in this article.

Read the rest here:

Global Law Enforcement, Security Firms Team Up, Take Down Shylock

By Sara Peters, Dark Reading, July 10, 2014

Come home to a hot iron and smoldering clothes this afternoon? Soon, it may not be a sign of forgetfulness, but rather evidence that you’ve been hacked.

A month after the GameOver ZeuS sting, another bank fraud group’s operations has been disrupted by an international collaboration of security firms and law enforcement agencies. The new target is Shylock, a Trojan that has stolen from banks in the U.S., Italy, and especially the United Kingdom.

Today the U.K.’s National Crime Agency (NCA) announced that it has seized Shylock operators’ command-and-control servers and taken control of the domains they use to communicate. The effort was led by NCA, and included the FBI, the European Cybercrime Centre at Europol, GCHQ, BAE Systems Applied Intelligence, Dell SecureWorks, Kaspersky Lab, the German Federal Police, and others in Italy, Turkey, France, Poland, and the Netherlands.

"The NCA is coordinating an international response to a cyber crime threat to businesses and individuals around the world," said Andy Archibald, Deputy Director of the NCA’s National Cyber Crime Unit, in a statement. "This phase of activity is intended to have a significant effect on the Shylock infrastructure, and demonstrates how we are using partnerships across sectors and across national boundaries to cut cyber crime impacting the UK."

"The European Cybercrime Centre (EC3) is very happy about this operation against sophisticated malware, playing a crucial role in the work to take down the criminal infrastructure," said Troels Oerting, head of the European Cybercrime Centre (EC3) at Europol, in a statement. "EC3 has provided a unique platform and operational rooms equipped with state-of-the-art technical infrastructure and secure communication means, as well as cyber analysts and cyber experts. In this way we have been able to support frontline cyber investigators."

Shylock, first discovered in 2011, is so named after the character Shylock in Shakespeare’s "The Merchant of Venice," because the malware’s code contains lines from the play. In March, Dell SecureWorks named Shylock one of the Top Banking Botnets of 2013, citing that it was responsible for 7% of the banking malware it detected (behind only GameOver ZeuS, Citadel, and other variants of ZeuS).

Symantec estimates that the gang behind Shylock has stolen several million dollars from victims over the past three years. Over 60,000 infections were detected in the past year. Shylock spreads through a wide variety of vectors, including phishing messages, "malvertising," malicious PDFs, drive-by downloads, fake browser updates, removable media devices, Skype instant messages, and man-in-the-browser attacks. It uses several exploit kits, including Blackhole, Cool, Magnitude, Nuclear, and Styx.

According to Symantec, Shylock uses a technique termed automated-transaction-service (ATS), which can automatically send a logged-in user’s credentials to the attacker and initiate fraudulent transactions in the background. It can hide its tracks by modifying account balances and transaction records or adjusting percentages and values of funds to evade fraud detection logic.

It’s proven itself capable of defeating banks’ two-factor authentication. In some cases, the attackers posed as bank representatives, opening chat windows to talk to customers and directly request all the account information needed to transfer money from the customer’s account to another one held by the criminals. They even distract users, if necessary, by popping up phony security alerts.

According to NCA, "Intelligence suggests that Shylock has to date targeted the UK more than any other country, although the suspected developers are based elsewhere."

Symantec estimates that the UK is Shylock’s largest target by far, claiming about 30% of the attackers’ efforts over the past year. Why? As Symantec explains:

Despite high infection numbers, the attackers have maintained a very narrow geographical focus. The UK is by far its largest target. The country has a large banking customer base, a high online banking adoption rate, and a high number of wealthy citizens. The UK also has a relatively small number of banks relative to its size. Since the attackers have to tailor the malware to perform attacks on individual banks, this makes the UK market doubly attractive.

Read the rest here: http://www.darkreading.com/global-law-enforcement-security-firms-team-up-take-down-shylock/d/d-id/1297194?
Senate Hearing Calls For Changes To Cybercrime Law

By Sara Peters, Dark Reading, July 16, 2014

Law enforcement agencies across the globe are taking a page out of the cybercriminal handbook, using targets’ own phones and computers to spy on them with methods traditionally associated with the world’s most malicious hackers, two computer security groups say.

Panelists on a Senate Judicial Committee hearing yesterday called for changes to the Computer Fraud and Abuse Act (CFAA) and other legislation that addresses cybercrime. The hearing, titled “Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks,” was organized in the wake of Microsoft’s botnet takedown that also took down some non-criminal customers of No-IP.

The conversation was about fighting botnets in general -- No-IP itself was never mentioned by name. It was, however, briefly implied by panelist Craig D. Spiezle, executive director and founder of the Online Trust Alliance:

Botnet take-downs and related efforts need to be taken with care and respect to three major considerations: the risk of collateral damage to innocent third parties, errors in identifying targets for mitigation, and respecting users’ privacy. For example, taking down an entire web hoster because they have a handful of bad customers may be an example of unacceptable collateral damage. At the same time hosters and ISPs cannot hide behind bad actors and must take reasonable steps to help prevent the harboring of criminals and enabling cybercrime activity.

The panel also included Richard Domingues Boscovich, assistant general counsel of Microsoft’s Digital Crimes Unit, which led the seizure of No-IP servers and domains.

"Microsoft's philosophy to fighting botnets is simple. We aim for their wallets," he said. "We disrupt botnets by undermining cyber criminals' ability to profit from malicious attacks."

However, going after "their wallets," is not always easy. Security professionals (in tandem with law enforcement) can use technological means to disrupt criminal infrastructure, but when it comes to prosecuting the perpetrators at the center of that black market, the law can fall short.

Therefore, Domingues Boscovich expressed support for some of the law amendments proposed by panelist Leslie Caldwell, assistant attorney general of the US Department of Justice's Criminal Division.

One of Caldwell’s suggestions: Add a piece to the CFAA -- which has not been amended since 2008 -- that directly criminalizes the trafficking of botnets. That way the people selling the botnets for other people to use could also be held accountable for their role in the criminal infrastructure.

Another suggestion was to amend the Access Device Fraud statute. The statute currently allows prosecutors to bring charges against the perpetrators of phishing and credit card fraud schemes if they’re based in the United States, but does not apply to offenders in foreign countries. Caldwell recommends that the overseas sale of stolen US financial information be criminalized.

Another suggestion is to amend the CFAA to eliminate the requirement to prove intent to defraud. As Caldwell explained, "Such intent is often difficult -- if not impossible -- to prove because the traffickers of unauthorized access to computers may have a wrongful purpose other than the commission of fraud. Indeed, sometimes they may not know or care why their customers are seeking unauthorized access to other people's computers."

Any suggestion to remove the need to prove intent, however, gets tricky.

Read the rest here:
http://www.darkreading.com/senate-hearing-calls-for-changes-to-cybercrime-law/d/d-id/1297331?
The dangers of social media
(in the military)

By Lance Cpl. Tyler Giguere, DVIDS, July 17, 2014

The explosive growth in both the use and capacity of smartphones has led to a sea change in digital forensics, creating technology challenges for the justice and law enforcement communities and raising legal questions that in some cases have gone to the Supreme Court.

A Marine is using social media when a female he does not recognize sends him a friend request. He enjoys meeting new people, so he accepts her request. They begin to chat and soon decide to meet. Before they meet, she tells the Marine he must contact, a man who knows the woman. The man tells him he must pay money or the Marine and his family and friends will be in danger.

Common tactics of social media extortionists include relating to a service member's interests and posting pictures of attractive females to lure them into chats. What may seem like a normal person wanting to video chat or meet with a Marine, can actually be an extortionist trying to deceive him for his money or information.

Extortion became a noticeable issue for Naval Criminal Investigative Service Resident Agency, Okinawa, Japan, in 2012. Since then, cases have become five times more frequent, with more than 25 investigations and reports being taken, and have led to monetary losses of nearly $20,000, according to Special Agent Doug Simmons, a criminal investigator with NCISRA, Okinawa.

"The Marine Corps is a strong mannered, strong willed, cultured community, so they are more reluctant to report that they have been a victim of a crime," said Simmons.

Embarrassment about their information being made public could be a reason why only some Marines report the incidents, according to Staff Sgt. Christopher I. Cureton.

"People are not coming forward because they do not want their information (made public)," said Cureton, the cyber security chief for Marine Corps Installations Pacific-Marine Corps Base Camp Butler. "But we offer preventative measures to protect your information. Privacy of Marines is our main purpose."

Extortionists are able to search for the common words "Marine," "United States Marine," "USMC" and find anyone on social media sites with low privacy settings whose profile page includes those words. They then add the Marine, who might confirm them as a friend based on mutual friends or the photos posted to the profile.

"Just because they have mutual friends with someone does not make them real," said Simmons. "Quiz them. Ask questions such as, ‘where did we meet?’ If they say they are military ask, ‘What platoon were we in? Where were we trained?’"

Being on Okinawa makes the extortionist threat even more realistic as it is easy for criminals to portray themselves as Okinawa residents before demanding money be sent to the Philippines or another country around the Asia-Pacific, according to Simmons.

“When threats are being made against Marines, or their family and friends, it is recommended that service members keep and archive any electronic evidence, paper documentation, conversations and emails between you and the suspect.”

“I protect not only myself, but other people on social media,” said Lance Cpl. Kel V. Blaze, combat camera, G-3/5, operations and training, MCIPAC-MCB Butler. “I report the fake accounts or show the accounts to the public and say, ‘Hey, watch out for this profile because they are not real.’”

Read the rest here:
http://www.dvidshub.net/news/136671/dangers-social-media#.U97w3iUg-Uk

Snowden to Hackers of the World: Build NSA-proof Systems

By Info-Security magazine, July 22, 2014

NSA whistleblower Edward Snowden has called on designers, developers and technologists across the globe to build communications systems which can shut out prying state-sponsored snoopers.

Speaking via an online link up from Russia at the Hope X hacker conference in New York, Snowden responded to a question from a Twitter user around what those in technology can do to "make things better”.

“When I talk about this I say ‘encryption; encryption, encryption, encryption’, because it’s an important first step,” he said.

Warning that the same tools techniques used by governments to detect spies are employed to root out troublesome journalists, he called on technologists passionate about freedom of speech and protecting civil liberties to join forces in developing NSA-proof systems.

Read the rest here:
Report Connected devices have huge security holes

By Phys.org, July 29, 2014

The surge of Web-connected devices—TVs, refrigerators, thermostats, door locks and more—has opened up huge opportunities for cyberattacks because of weak security, researchers said Tuesday.

A study by the Hewlett-Packard security unit Fortify found 70 percent of the most commonly used "Internet of Things" devices contain vulnerabilities, including inadequate passwords or encryption, or lax access restrictions.

"While the Internet of Things will connect and unify countless objects and systems, it also presents a significant challenge in fending off the adversary given the expanded attack surface," said Mike Armistead, vice president and general manager for Fortify's enterprise security.

"With the continued adoption of connected devices, it is more important than ever to build security into these products from the beginning to disrupt the adversary and avoid exposing consumers to serious threats."

The study comes amid recent security warnings about hacking of medical devices, cars, televisions and even toilets that have an Internet connection.

The researcher scanned the most popular devices and their cloud components and found on average 25 vulnerabilities per device. These products included TVs, webcams, home thermostats, remote power outlets, sprinkler controllers, hubs for controlling multiple devices, door locks, home alarms, scales and garage door openers.

The study said eight of 10 devices tests leaked private information that could include the user's name, email address, home address, date of birth, credit card or health information.

Most of the devices lacked passwords, making it easier for hackers or others to gain access while some included simple default passwords such as "1234."

Some 70 percent of the devices analyzed failed to use encryption for communicating with the Internet and local network, another weakness that makes for easy outside access.

Read the rest here:

Upcoming Chapter Meetings

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sept. 9</td>
<td>10:45 to 1:00</td>
<td>The Retired Enlisted Association 834 Emory Circle (719) 596-0927</td>
</tr>
<tr>
<td>Sept. 18</td>
<td>5:45 to 8:00</td>
<td>TREA</td>
</tr>
<tr>
<td>TBD</td>
<td>TBD</td>
<td>October Conference at UCCS</td>
</tr>
<tr>
<td>Nov. 12</td>
<td>10:45 to 1:00</td>
<td>TREA</td>
</tr>
</tbody>
</table>

*No evening meeting in November*

| TBD | 10:45 to 1:00 | Holiday Luncheon—Location TBD |

Upcoming Chapter Meetings

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sept. 9</td>
<td>10:45 to 1:00</td>
<td>The Retired Enlisted Association 834 Emory Circle (719) 596-0927</td>
</tr>
<tr>
<td>Sept. 18</td>
<td>5:45 to 8:00</td>
<td>TREA</td>
</tr>
<tr>
<td>TBD</td>
<td>TBD</td>
<td>October Conference at UCCS</td>
</tr>
<tr>
<td>Nov. 12</td>
<td>10:45 to 1:00</td>
<td>TREA</td>
</tr>
</tbody>
</table>

*No evening meeting in November*

| TBD | 10:45 to 1:00 | Holiday Luncheon—Location TBD |
ISSA meeting photos are courtesy of our Chapter photographer Warren Pearce.

Presentation of Chapter Coins.

And more coins!
The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Article for the Newsletter?
If you would like to submit an article...

Are you a budding journalist? Do you have something that the Colorado Springs ISSA community should know about? Can you interview one of the “movers and shakers”? Tell us about it!

We are always looking for articles that may be of interest to the broader Colorado Springs security community.

Send your article ideas to Don Creamer at:

doncreamer-issa@q.com

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

Guy brags about gift card tinkering at new job, gets house raided by feds

By Lisa Vaas, Naked Security, July 30, 2014

Three years ago, Muneeb Akhter and his twin brother Sohaib, then 19 years old, were featured in the Washington Post in a story headlined "George Mason's youngest grads."

They had graduated from George Mason University, in Washington, DC, with degrees in electrical engineering - "arguably the school's toughest program", the Post noted - after three years.

They reportedly liked to invent robots.

"I think we'll be hearing more about these guys", the Post's Tom Jackman wrote.

Yes, indeed, starting now.