ASK Technologies, Inc.

SPRING 2016

Volume 16 Issue 1

ASK NEWS

In this edition of ***ASK News***, we discuss email encryption, email scams and our new relationship with Layer 8 Security. Once again, we are also proud to be the recipient of the Philadelphia Business Journal's Top 25 Systems Integrators and Top 25 Software Developers awards—and new this year, we have been recognized as one of the Top 25 Computer Consultants in our area. ASK has also reached top Premier Partner status with Datto, ensuring our clients receive the most competitive pricing and support levels available. This is an exciting time for ASK. Enjoy this edition of ASK News.

Stephen Pirolli, ASK Technologies, Inc.

Inside this issue:

WELCOME NEW CLIENTS

McKean Defense Group

Cardinal Systems, Inc.

Trenton Country Club 1897

Newtown Township 1683 Bucks County, Pennsylvania

Email Encryption by ZixCorp

From our Sales Team

Email Encryption is hot right now.

You may have seen a lot of encryption news lately, and you aren't alone. According to Hoffman & Hoffman Worldwide the level of interest in encryption and the number of encryption-related news articles are at an all-time high. What's causing all the attention? A few things:

Increased Breaches

When a breach occurs, the loss of customers' trust is not only damaging to the company's reputation, but also to their bottom line. According to the Ponemon Institute's report, the average cost of a security breach is $3.5 million. Data breach costs include direct expenses like engaging forensic experts and discounts for future products and services, as well as indirect costs like internal investigations, communications, and the extrapolated value of customer loss from turnover or reduced customer acquisition rates.

The cost of a breach, both in dollars and time, far exceeds the cost of prevention.

Increased Audits

The Office of Civil Rights (OCR) is responsible for enforcing HIPAA regulations and they have publicly announced a renewed focus on audits, saying that past audits will "pale in comparison" to the enforcement ahead.

continued on pg. 2

BALA CYNWYD, PA — MAY 2016:
ASK TECHNOLOGIES, INC. is once again a proud recipient of the Philadelphia Business Journal's prestigious awards for "Top 25 Systems Integrators" and "Top 25 Software Developers", and new this year, "Top 25 Computer Consultants". This marks the thirteenth consecutive year that ***ASK TECHNOLOGIES, INC.*** has been recognized as an industry leader in the Philadelphia and Metropolitan Area.

As Published In
Philadelphia Business Journal
April 2016
TOP
SYSTEM INTEGRATORS,
COMPUTER CONSULTANTS
& SOFTWARE DEVELOPERS
2 0 1 6
ASK Technologies
Top System Integrators, Computer Consultants & Software Developers
Philadelphia Business Journal - April 2016

ASK provides our clients the ability to transform current information technology into productivity. Whether utilizing technology to bridge the gap between employees, business workflow and computers, or using technology to supply access to data, regardless of connection, location and time, ***ASK*** offers the solutions you need to survive in a very competitive world.

ASK Receives Premier Partner Status with Datto

From our Sales Team

Effective April 1, 2016, Datto, the industry leader in providing remote backup and business continuity solutions, has recognized ***ASK Technologies, Inc.*** as a Premier Partner serving the PA, NJ and NY areas.

"ASK is very excited about our new, upgraded partner level designation with Datto," says Stephen F. Pirolli, ASK Technologies, Inc. "Datto's award winning solutions and 7x24 support are the best the industry has to offer, providing both small and large clients with a true premise and cloud business continuity strategy. ASK's new Premier Partner status will allow us to grow our relationship with Datto even further," continued Pirolli.

"ASK Technologies has joined a select group of IT firms in achieving Datto's Premier Partner status," said Aaron Perry, Datto. "Having a Premier Partner status with Datto will further enable ASK Technologies to deliver and support Datto's entire suite of products and services while also benefiting from Datto's most competitive pricing," said Perry.

ASK Technologies, Inc. is a national provider of IT hardware, software and professional services with proven experience and expertise in various technology areas, stretching across multiple vertical markets. With a specialization in multi-service network integration, ***ASK*** creates innovative and cost effective solutions to solve our clients' mission critical business needs.

Datto is an innovative provider of comprehensive backup, recovery and business continuity solutions used by thousands of managed service providers worldwide. Datto's 190+ PB purpose-built cloud and family of software and hardware devices provide Total Data Protection everywhere business data lives, for businesses of every size.

Email Encryption by ZixCorp

Continued from pg. 1

Strengthened Regulations

Securing sensitive information in email for customers, partners and employees isn't just a best practice — it's often the law. As of June 2014, there were 47 states with their own data security/ breach notification laws. As time goes by, the laws continue to get stricter.

The list of reasons to be concerned about security breaches is long and daunting, however the solutions are simple. We recommend joining the Zix Encryption Network. It's a growing community of more than 10,000 customers that enables the automatic exchange of encrypted email for all messages between members. The best part is email sent to other members are delivered transparently; no portals or passwords, just email.

Whether it is customer data, partner data or intellectual property, no industry is exempt from the need to protect their company's sensitive information. In addition, no company can deny that email continues to be the preferred method of business communication.

Contact your local ***ASK*** sales rep at (610) 617-0300 to learn just how simple email encryption can be, with ZixCorp Email Security Services.

With ZixCorp Email Security Services, you can trust that:

- ***Customer information is secure***
- ***Your reputation is protected***
- ***Email exchange complies with federal and state regulations***
- ***Your most valuable relationships with customers and partners are not jeopardized by data breaches in email***
- ***Company assets are protected from being sent through email***

Still Waiting for Windows 10?

From our Tech Staff

Still waiting for Windows 10? You can jumpstart the upgrade by pointing your browser to https://www.microsoft.com/en-us/software-download/windows10. Near the bottom of the page are two options – a 32-bit tool, and a 64-bit tool. If you are upgrading form Windows 7 or 8, the upgrade is free. If you are running the Enterprise version of either product, then you'll need to purchase the appropriate license.

To upgrade, download the appropriate tool. You can't use this tool to upgrade form 32-bit to 64-bit – you need to download the tool that's appropriate for your OS. It only takes a few seconds to download the tool, but don't be fooled. Upgrading your machine is going to take anywhere from three to four hours.

Once you have the appropriate tool downloaded, run it. You will have one of two options – Upgrade the local machine, or download for upgrading a different machine. If you select the download option, you will be downloading the Windows 10 ISO file. This file can be burned (using an appropriate tool, like IMG Burn) to a DVD, and then used in the traditional way to upgrade a machine. But be warned, upgrading a machine this way still takes time.

Before you upgrade, you should make a backup of your system. We suggest backing up all important files to an external USB drive. Then, create a system image (we can help you do that if you don't know how – just give us a call).

One more thing to do before you start the upgrade. Unplug any USB devices you have attached. The only thing your PC should have plugged in is the monitor, keyboard, and mouse. If the upgrade has to deal with a peripheral, there is a good likelihood the upgrade may fail. Some users have even stated they needed to disconnect all but their primary hard drive.

The install process first copies over the files needed to do the install. It then creates a system restore point. This is a good thing in that if the install fails, the system can revert back to the way it is now. The first time we did an upgrade, it failed, and we were very happy to not lose anything. The upgrade process will run some tests, and then reboot.

continued on pg. 4

"Before you upgrade, you should make a backup of your system. We suggest backing up all important files to an external USB drive. Then, create a system image (we can help you do that if you don't know how – just give us a call)."

Claim Your Free 1TB of Cloud Storage | Datto Drive

From our Sales Team

ASK would like to invite you to try out Datto Drive, a brand new file storage platform built by our business partner Datto.

Datto Drive is a best-in-class file sync & share tool that will allow your team to store and collaborate on all of your files and projects from any operating system or mobile device.

Best of all, for the next year, 1 TB of cloud storage space is available for FREE to the first one million Datto Drive customers. As a Datto Premier Partner, we are able to provide you early access to this incredible offer.

To claim your 1 TB of free cloud storage today, click here to sign up your business for Datto Drive.

Questions? Contact your local ***ASK*** sales rep today at (610) 617-0300 to learn more about the free 1TB of cloud storage being offered by Datto.

"Best of all, for the next year, 1 TB of cloud storage space is available for FREE …"

FBI: $2.3 Billion Lost to CEO Email Scams

As featured in Krebsonsecurity.com

The U.S. Federal Bureau of Investigation (FBI) this week warned about a "dramatic" increase in so-called "CEO fraud," e-mail scams in which the attacker spoofs a message from the boss and tricks someone at the organization into wiring funds to the fraudsters. The FBI estimates these scams have cost organizations more than $2.3 billion in losses over the past three years.

In an alert posted to its site, the FBI said that since January 2015, the agency has seen a 270 percent increase in identified victims and exposed losses from CEO scams. The alert noted that law enforcement globally has received complaints from victims in every U.S. state, and in at least 79 countries.

CEO fraud usually begins with the thieves either phishing an executive and gaining access to that individual's inbox, or emailing employees from a look-alike domain name that is one or two letters off from the target company's true domain name. For example, if the target company's domain was "example.com" the thieves might register "examp1e.com" (substituting the letter "L" for the numeral 1) or "example.co," and send messages from that domain.

Unlike traditional phishing scams, spoofed emails used in CEO fraud schemes rarely set off spam traps because these are targeted phishing scams that are not mass e-mailed. Also, the crooks behind them take the time to understand the target organization's relationships, activities, interests and travel and/or purchasing plans.

They do this by scraping employee email addresses and other information from the target's Web site to help make the missives more convincing. In the case where executives or employees have their inboxes compromised by the thieves, the crooks will scour the victim's email correspondence for certain words that might reveal whether the company routinely deals with wire transfers — searching for messages with key words like "invoice," "deposit" and "president."

On the surface, business email compromise scams may seem unsophisticated relative to moneymaking schemes that involve complex malicious software, such as Dyre and ZeuS.

continued on pg. 5

"Unlike traditional phishing scams, spoofed emails used in CEO fraud schemes rarely set off spam traps because these are targeted phishing scams that are not mass e-mailed."

Still Waiting for Windows 10?

continued from pg. 3

You'll be faced with a big circle on the screen – to show the upgrade status, and three categories down below. The system may or may not reboot between each of these three stages. After the final boot, the system will display the new, fancy logon screen. From this point forward, it functions similar to Windows 8, except it boots directly to the desktop screen.

And that's all there is – one of the simplest upgrades we've ever seen. And from our experience so far, Windows 10 is faster and much more efficient than any of the previous versions of Windows. In future posts, we'll be discussing some of the new features, as well as Windows latest browser, Edge.

As always, should you have any questions, or concerns, or need assistance, give us a shout. We're only a phone call away.

"...from our experience so far, Windows 10 is faster and much more efficient than any of the previous versions of Windows."

FBI: $2.3 Billion Lost to CEO Email Scams

Continued from Page 4

But in many ways, CEO fraud is more versatile and adept at sidestepping basic security strategies used by banks and their customers to minimize risks associated with account takeovers. In traditional phishing scams, the attackers interact with the victim's bank directly, but in the CEO scam the crooks trick the victim into doing that for them.

The FBI estimates that organizations victimized by CEO fraud attacks lose on average between $25,000 and $75,000. But some CEO fraud incidents over the past year have cost victim companies millions — if not tens of millions — of dollars.

Last month, the Associated Press wrote that toymaker Mattel lost $3 million in 2015 thanks to a CEO fraud phishing scam. In 2015, tech firm Ubiquiti disclosed in a quarterly financial report that it suffered a whopping $46.7 million hit because of a CEO fraud scam. In February 2015, email con artists made off with $17.2 million from The Scoular Co., an employee-owned commodities trader. More recently, I wrote about a slightly more complex CEO fraud scheme that incorporated a phony phone call from a phisher posing as an accountant at KPMG.

The FBI urges businesses to adopt two-step or two-factor authentication for email, where available, and to establish other communication channels — such as telephone calls — to verify significant transactions. Businesses are also advised to exercise restraint when publishing information about employee activities on their Web sites or through social media, as attackers perpetrating these schemes often will try to discover information about when executives at the targeted organization will be traveling or otherwise out of the office.

For an example of what some of these CEO fraud scams look like, check out this post from security education and awareness firm Phishme about scam artists trying to target the company's leadership.

Continued on pg. 6

"The FBI estimates that organizations victimized by CEO fraud attacks lose on average between $25,000 and $75,000. But some CEO fraud incidents over the past year have cost victim companies millions — if not tens of millions — of dollars."

ASK Technologies Partners With Layer 8 Security

From our Sales Team

ASK Technologies, Inc. is proud to announce its newly established partnership with Layer 8 Security to bring the latest in cybersecurity advisory and technical services to the Greater Philadelphia area. They focus on the effective management of cybersecurity at the human layer where business processes and technology intersect. The Layer 8 Security team has extensive experience and training from operations serving the National Security Agency, U.S. Cyber Command, Department of Defense, Special Operations, and Defense and Private Industries.

Part of the value Layer 8 Security brings to ***ASK Technologies'*** clients is information about the most recent cybersecurity threats and mitigation techniques. They recently presented at the inaugural Technology Leaders Forum hosted by Rittenhouse Ventures at the Navy Yard where Chief Technology Officers and senior leaders of local companies received the latest in data security strategies, technical tactics, and training policies that pertain to cybersecurity.

Continued on pg. 6

layer8security

Cybersecurity is no longer just an IT issue, it is a critical business issue that requires a focus on integrating security into all aspects of your people and business processes.

The Layer 8 Security philosophy is focused on the human layer of cybersecurity, where business processes and technology intersect.

ASK technologies, inc.

ASK TECHNOLOGIES, INC.

Creating new standards in multi-service network integration.

ASK Technologies, Inc.

7 Bala Avenue
Suite 201
Bala Cynwyd, PA 19004

610-617-0300 Office
610-617-0307 Fax
info@asktech.com

*For operational excellence at predictable costs, turn to **ASK**.*

FBI: $2.3 Billion Lost to CEO Email Scams

Continued from Page 5

I'm always amazed when I hear security professionals I know and respect make comments suggesting that phishing and spam are solved problems. The right mix of blacklisting and email validation regimes like DKIM and SPF can block the vast majority of this junk, these experts argue.

But CEO fraud attacks succeed because they rely almost entirely on tricking employees into ignoring or sidestepping some very basic security precautions. Educating employees so that they are less likely to fall for these scams won't block all social engineering attacks, but it should help. Remember, the attackers are constantly testing users' security awareness. Organizations might as well be doing the same, using periodic tests to identify problematic users and to place additional security controls on those individuals.

ASK Technologies Partners With Layer 8 Security

Continued from Page 5

Key Concerns of the Audience

Leaders of these area companies wanted to know how to account for data if it is moved or a screen capture is taken. How do they streamline the effort in responding to assessments and/or requirements from third parties? Should businesses be testing software applications for vulnerabilities and shortcomings? Encryption of data-at-rest is important, but do companies implement that in their network or at the end-user level? Companies need to balance security and usability for employees, but feel like security is taking over, how do they balance it?

The Bottom Line to Address These Concerns: Every business needs these solutions in place

- Education on cybersecurity defensive strategies and tactics to your employees
- Identify the different types of cyber threats to your employees
- Layered defenses: people, processes, technology, insurance all create a safe environment
- Compliance requirements from clients or government associations are growing- know yours
- Create a cybersecurity information management program that encompasses all of the above and put someone in charge.

To learn how your business can be more resilient against cyber attacks and other threats, contact your ***ASK*** Sales Rep at (610) 617-0300.

SHORT CUTS
New for Windows 10

Windows
Show the Windows 10 Start Menu

Windows + Tab
Launch Windows 10 Task View

Windows + I
Open Windows 10 settings

Windows + Ctrl + D
Create new virtual desktop

Windows + X Open
Start button context menu