All the latest technology trends and topical issues

NOV/DEC 2015

technology times

New Cyber Security book co-authored by Stuart Sanders

VACATION ALERT

Dangers of Using Public Wifi Hot Spots

The FIVE MOST Dangerous Pieces of Information

Velocity Technology

Contents Nov/Dec 2015

5 Featured Fund Management Software

6 Is your Company's data at Risk?

7 How to make yourself "Invisible" to hackers

8 The Cyber Security Challenge

HK Newsletter Team

Stuart Sanders
EDITOR

Michael Early
EDITOR IN CHIEF

Cristina Caratao
ART EDITOR

Gonzalo Sanchez
ASSISTANT ART EDITOR

Newsletter Contact

newsletter@velocity-technology.com
+852 2915.5096
+852 2834.8852

STUART'S CORNER

> "As a business owner, you don't have time to waste on technical and operational issues. That's where we shine!"

Welcome everyone to the new look of our technology times newsletter. It has been a few months since the last one which was a much simpler and smaller edition. We are currently planning to publish this newsletter every 2 months, and the next issue is due in the 2nd week of January.

This edition is primarily focused around digital security issues. You'll find articles on how to protect yourself, what information criminals are after, products that help detect attacks and those that help recover from an attack. We also have an article about the recent cybersecurity event we co-sponsored along with KPMG, EMC and the Canadian Chamber of Commerce.

So far this has been a good year for us. Business expansion has been good and we have widened our alliances and partnerships with other providers supporting the banking and finance industries, particularly the hedge fund space. The support team has expanded considerably and we have additions in both our sales and marketing teams.

Finally take a look on page 5. I am a contributing author to a book due to be released early next year and you can find out more details.

Wishing everyone a good finish to the year and if you are taking holidays enjoy what will surely be a well earned break.

STUART SANDERS
Managing Director
Velocity Technology

stuart.sanders@velocity-technology.com
Velocity Technology Limited
Velocity Technology Limited
VelocityTechnologyLimited
@velocitytechhk

COVER STORY

The Five Most Dangerous Pieces of Information

In the book Spam Nation, investigative journalist and cybersecurity expert Brian Krebs revealed the single most effective (and relied upon) way cybercrime rings gain access to your bank account, credit cards and identity. Ready for it? E-MAIL.

Whether it's opening an attachment infected by a virus, or a phishing scam where you unknowingly give up your login to a critical web site, e-mail still remains the most popular and reliable way digital thieves can rob you blind, steal your identity and wreak havoc on your network. Worst of all? You're inviting them in! While there are a number of things you need to do to protect yourself, here are five pieces of information you (and your team) should never put in an e-mail.

Your HK ID#. Think of this as your "bank account" number with the government. You should never e-mail this to anyone because it can be used to open credit cards and steal your identity.

Banking information. Your bank account numbers, routing number and online banking login credentials should never be e-mailed. Further, avoid sending a voided, blank check as an attachment to an e-mail.

Your credit and/or debit card information. Never update a credit card via an e-mail! If you need to update a card with a vendor, there are two safe ways to do this. The first is to log in to your vendor's secured site by going to the URL and logging in. Do not click on a link in an e-mail to go to any web site to update your account password or credit card! Hackers are masters at creating very legit-looking e-mails designed to fool you into logging in to their spoof site, which looks very similar to a trusted web site, to enter your username, password and other financial details, thereby gaining access. Another way to update your account is to simply call the vendor direct.

Login credentials and passwords. You should never share your passwords or answers to security questions with anyone for any site, period.

Financial documents. An attachment that includes any of the above is just as dangerous to e-mail as typing it in. Never e-mail any type of financial documents (or scans of documents) to your CPA, financial advisor, bank, etc.

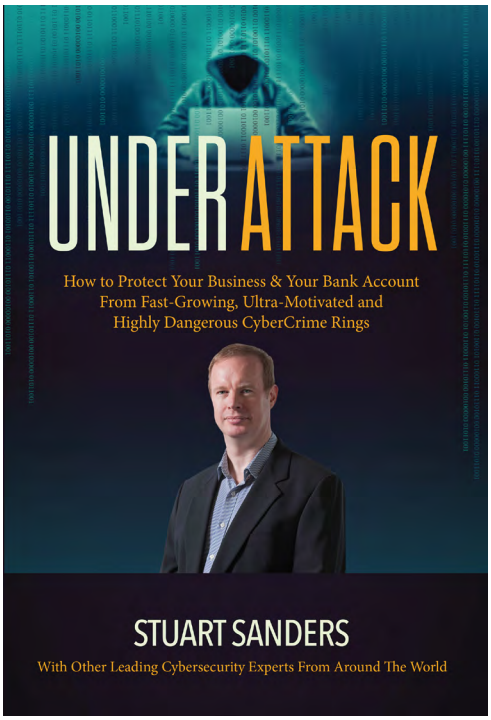
Remember: Banks, credit card companies and the government will never ask you to click a link to provide them with any of the five items above. If you get an e-mail requesting you to update any of the above information, there's a good chance it's a phishing e-mail from a hacker. Don't be fooled!

For a free risk assessment contact us at **sales@velocity-solutions.com**

New Cybersecurity book co-authored by Stuart Sanders

> Stuart Sanders teamed with 26 leading cyber security experts from around the world to release the new book, "Under Attack: How To Protect Your Business and Your Bank Account From Fast-Growing, Ultra-Motivated and Highly Dangerous Cybercrime Rings" by CelebrityPress."

I'm happy to announce that I am a co-author in an upcoming book on cyber security. This is a book that has been a year in the planning and one that I was invited to contribute to earlier this year. The picture to the right is the cover of the special edition we will be ordering for Hong Kong.



The wording "Under Attack" implies a dangerous situation – one that signifies we are currently under assault. This is more so today than ever before. Just this week as we put the final touches on the newsletter, there has been several newsworthy items from the bad guys to attack individuals, businesses and online stores. Feel free to contact me if you want to be kept up to date on these kinds of issues.

There are very few businesses, organizations or even individuals left in Modern society that don't use electronics today. Even in Third World countries having a mobile phone (not necessarily a smart phone) is becoming the norm. The electronic Revolution has been all-encompassing. Remaining vestiges of "old world" practices – like manually writing or recording transactions or events, or the time-honored tradition of 'hiding money under the mattress' – have all but disappeared. So along with the use of bows and arrows and pony dispatch riders, these are becoming historical markers strewn along the path of progress.

The book covers a range of topics around the ever growing field of securing our digital assets. From cloud computing, data storage, managed security providers and more. If you are interested in the book let me know and I will happy to give you more details or reserve a copy post release.

In the coming months this is one of a number of initiatives we will have around cyber security and protecting your business. Stay tuned...

Stuart

PS. Feel free to contact me at stuart.sanders@velocity-solutions.com to learn more.

Cybercriminals Now Have A Bull's-Eye On Small Business...

Is Your Company's Data At Risk?

In a December 2014 survey by the National Small Business Association, 61% of small businesses reported being victims of a cybercrime within the past 12 months.

The average cost to recover from a cyber-attack skyrocketed from US$8,699 per attack in 2013 to US$20,752 per attack in 2014. And, of the businesses targeted, 68% said they'd been hacked more than once.

Experts agree, as cybercrooks become ever more sophisticated, the threat to small businesses is going to get worse before it gets better...

So what can you do to beat the bad guys?

Here are three common ploys used by hackers – and how you can fend them off:

1. **Phishing** – A really legitimate-looking e-mail urges you to click a link or open a file that triggers a malware installation on your computer.

   Best Defense: Don't let anyone in your company open files or click links in an e-mail unless they're certain who it came from.

2. Cracking Your Password – Hackers can run programs 24/7 testing password combinations. The easier your password is to guess, the more likely it is they'll crack it.

   Best Defense: Make sure your browser is up-to-date, or use one that updates automatically, such as Firefox or Chrome. Internet Explorer users have been found to be most vulnerable to these attacks.

3. Drive-By Download – You visit what appears to be an innocent site; yet when you click, your device gets hacked – and you may never know it, until it's too late.

   Best Defense: Consider using a password manager that generates and stores tough-to-crack passwords. For extra security, use unique passphrases for financial accounts in case the manager gets hacked.

Unfortunately, these three examples are just a small sampling of the dozens of ever more ingenious ways cybercriminals are breaking down the doors and destroying unprepared businesses.

How to Make Yourself Invisible to Hackers

There´s an old joke about two men hiking in the woods when they come across a big, grumpy black bear. Scared silly, one of the guys starts to run but notices his buddy stopped, bent-over, changing his shoes. He shouts to him, "What are you doing? Why aren´t you running?" to which his friend replies, "I´m changing my shoes because I don´t need to outrun the bear - I only need to outrun you."

This is a perfect analogy for what´s going on in small businesses: the "slow", easy targets are getting nailed by fast growing cybercrime rings that are getting more sophisticated and aggressive in attacking small businesses. Last year, the average cyber-attack cost North American small businesses US$20.752, a substantial increase from 2013, when the average was US$8.699. That´s because most small businesses don´t have security protocols in place or the manpower and budget to implement sophisticated security systems. While there´s absolutely no way to completely protect yourself other than disconnecting entirely from the Internet, there are several things you can do to avoid being easy pickings. Here´s how:

Lock your network. While wired networks make you invisible to WIFI snoops because you have to access them by plugging into physical outlets or hacking modem ports, you can create a hidden or cloaked network on a wireless network. Simply disable the service set identifier (SSID) broadcasting function on the wireless router, and only users with the exact network name will have access. Small businesses like coffeehouses can also do this - just periodically change the network´s information and place a small sign near the register with the current network name and passcode.

Encrypt your data. On your desktops, turn on the full-disk encryption tools that come standard on most operating systems: BitLocker on Windows-based PCs and FileVault on Macs. There is no noticeable performance lag; however, the encryption only applies when users have logged out the system. So setting computers to automatically log out after 15 minutes without use is a good idea. And for mobile devices, use a VPN (Virtual Private Network) to encrypt data traveling to and from your mobile devices and limit your employees access to only the company data that they must have to do their jobs.

Install best of breed firewall UTMs and anti-malware applications. On all of your equipment, including mobile devices.

Disable features that automatically connect your mobile devices to any available network.

Disable printer and file-sharing options on mobile devices before connecting to a hotspot.

Check before connecting to hotspots. If there is an unusual variation on the logo or name on the login page, beware... this could mean it´s a fake hotspot designed to steal your data.

KPMG Presents: The Cyber Security Challenge

October 22, 2015 - **Velocity** sponsored an event hosted by the Canadian Chamber of Commerce entitled **"KPMG Presents: Innovation and Technology Series Part 3- The Cyber Security Challenge"**.

As companies and organizations are experiencing cyber breaches with increasing sophistication, stealth, and persistence. The risk on cyber security is constantly rising, and yet many companies don't put more attention and investment to cyber security. The talk series covered the following topics: 1) The challenges of protecting financial information, customer data, and intellectual property. 2) The reputational and regulatory consequences of failing to do so? 3) The key elements of effective cyber risk oversight and governance.

One of the event speakers was Velocity solutions partner, Keith Glennan CEO of Tesserent. He has been in the IT industry for the past three decades and has worked in Australia and the United States for companies such as Hewlett-Packard and IBM. In 2012, Keith founded Tesserent a cyber-security company based in Australia. Tesserent provides managed security services for organizations across Asia Pacific.

Keith's topic was **"Cyber Security: Have we been asking the wrong question?"** Keith discussed the exponential growth of global detected and reported security incidents from 2009 to 2014. For the past decades, security breaches have become more resilient and sophisticated. Both private and government organizations have come under attack.

Examples of Security breaches include: 1) US Government/ US Office of Personal Management breached US government databases and stolen personal information on at least 21 million people, 2) eBay database of 145 million customers compromised, 3) Sony compromise personal records of employees

Organizations have become more aware of the cause of a breach in security, downtime in their business operation and loss of sensitive data. Security breaches are sometimes difficult to deal with in-house. As a result many of them are looking for managed security service providers (MSSPs) to ensure that their IT system is secure against potential breaches and cyber-attacks.

Keith Glennan - CEO, Tesserent

What should you consider in your MSSPs?

1. Implement user-centric security
2. Inspect your encrypted traffic
3. Inspect/ log application-level traffic
4. Implement or refine intrusion detection and IP reputation
5. Are you enforcing VPN's and using 2 Factor Authentication?
6. Review your policies and configuration

According to Keith, IT security is a business-level issue, not solely an IT issue. Management attention is required to protect sensitive business and personal information against unauthorized access.

FEATURED PRODUCTS

THE LATEST TECHNOLOGIES

STORAGECRAFT. SHADOWPROTECT® SPX

ShadowProtect® SPX is the newest addition to the StorageCraft Recovery Solution™. It provides enterprise-level backup and disaster recovery, data protection, and managed system migration for Windows and Linux systems on virtual and physical machines.

A disaster recovery solution that provides you with the products and services you need to recover your IT environment every time, everywhere, and from any disaster, great or small.

www.storagecraft.com/products/storagecraft-shadowprotect-spx

LogRhythm™ 7

LogRhythm, The Security Intelligence Company, recently unveiled LogRhythm 7, a major upgrade to its leading security intelligence andanalytics platform. New innovations in search, scalability, performance and security operations efficiencies will help organizations detect and respond faster to advanced cyber threats.

LogRhythm delivers immediate protection from security threats, compliance policy violations and operational issues with SmartResponse™. Intelligent, process-driven capabilities give organizations the power to automatically take action and respond to any alarm.

Version 7 of the LogRhythm security intelligence and analytics platform provides the visibility, automation and incident response orchestration capabilities required by the next-generation security operations center (SOC). The platform accomplishes this by collecting information from hundreds of thousands of disparate data sources, then analyzing and prioritizing the data and events. The resulting information becomes instantly available to SOC personnel.

www.logrhythm.com/logrhythm-7

Microsoft Surface Book is a Windows 10 device that redefines the laptop. The Surface Book combines high-end processing power with a best-in-class 13.5-inch PixelSense display that offers stunning clarity and resolution. The Surface Book provides exceptional power and versatility through features such as its 6th Generation Intel Core i5 or i7 processor with up to 16GB of memory, up to1 TB of storage, and an optional NVIDIA GeForce graphics chip.

Surface Book is more than a laptop—its detachable, 10-point multi-touch screen makes it a powerful clipboard as well.

https://www.microsoft.com/surface/en-us/devices/surface-book

Bluesmart is a high-quality carry-on suitcase that you can control from your phone, like a boss. From the app you can lock and unlock it, weigh it, track its location, be notified if you are leaving it behind and find out more about your travel habits. You can also charge your phone 6 times over with a built-in battery.

www.bluesmart.com

VACATION ALERT!

The One Thing You and Your Employees Should Never Do When On Vacation

This is the season when you and your team will be taking a little time off to head to the beach or your favorite vacation spot, and while we know we should completely disconnect from work, most of us will still check e-mail and do a little work while away - and that could end up causing some issues if you're not careful while working remote.

So before you head off to have a little fun with your laptop tucked under your arm, keep this in mind: never automatically connect to "any available network." Not all Internet connections are secure, so if you're going to log in to the company's network, e-mail or other critical cloud apps that are hosting sensitive information, only do so on a trusted, secured wifi and never a public one. We recommend investing in a personal Mifi device that acts as a mobile wifi hotspot if you're going to be traveling a lot and accessing company info.

Second, turn off the ability to automatically connect for all of your mobile devices and laptops. You will still be able to connect manually, but it will prevent your laptop or device from connecting to a questionable network without your consent or knowledge.

Finally, disable all printer and file-sharing options on your mobile devices. This is another way hackers can gain access to your network. In an ideal world, you and your employees would take a true break from work, but if they aren't able to completely detach themselves, then at least require them to stay safe using the above tips.

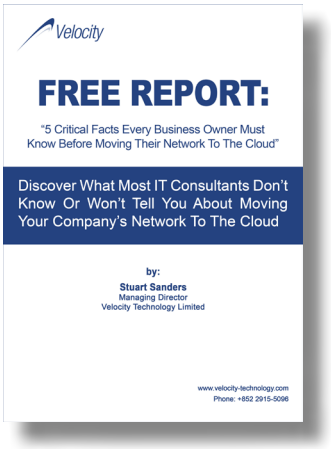
Free Report Download: If You Are Considering Cloud Computing For Your Company

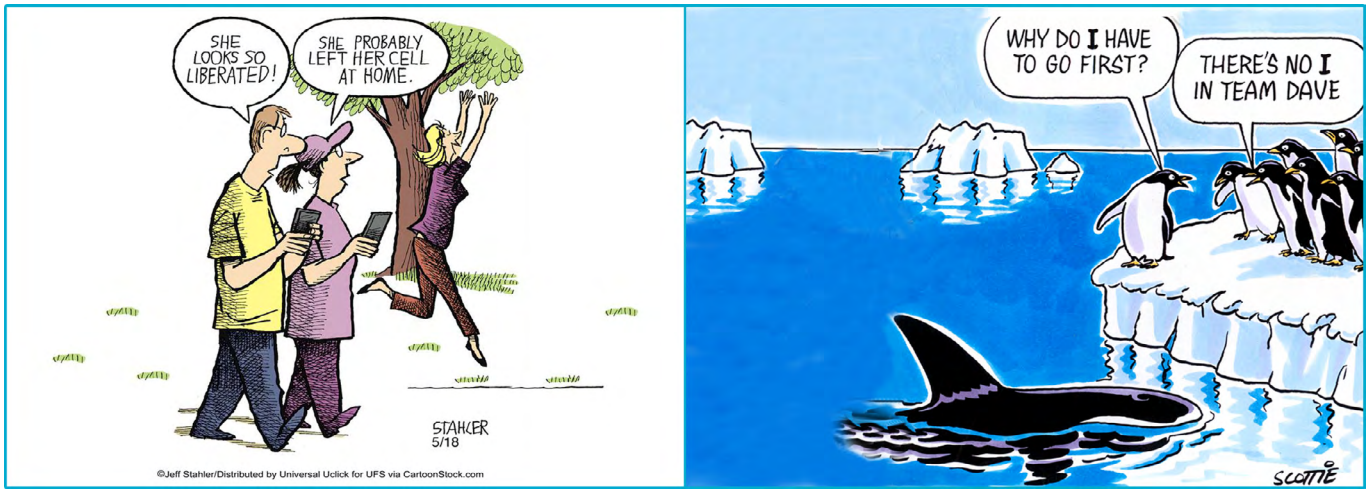
If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report, "5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."

This report discusses in simple, non-technical terms the pros and cons of cloud computing, data security, how to choose a cloud provider, as well as 3 little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated.

Even if you aren't ready to move to the cloud yet, this report will give you the right information and questions to ask when the time comes.

Get Your Free Copy Today: www.velocity-technology.com/cloudreport





Business Humour

Fresh out of business school, the young man answered a want ad for an accountant. Now he was being interviewed by a highly agitated, arrogant little man who ran a small business that he had started from scratch.

"I need someone with an accounting degree," the man said. "But mainly, I'm looking for someone to do my worrying for me."
"How's that?" the would-be accountant asked.
"I worry about a lot of things," the man said. "But I don't want to have to worry about money. Your job will be to take all the money worries off my back."
"I see," the accountant said. "And how much will my position pay?"
"I'll start you at 85,000," responded the owner decisively.
"Eighty-five thousand dollars!" the accountant exclaimed. "How can such a small business afford a sum like that?"
"That," the owner said, "is your first worry. Now get to work."

Who Else Wants to Win a HK$200 Starbucks Voucher?

For this issue of the newsletter we will give away a HK$200 Starbucks gift voucher to the first correct email sent to trivia@velocity-solutions.com.

The question for this issue is what is the longest road and rail suspension bridge in Hong Kong?

Email us now with your answer!

Velocity Technology provides first-class IT services to businesses that are looking to take advantage of new opportunities. With IT services that are matched to meet the specific needs of your business, you can enjoy the advantages of technology without the stress it often creates. Infrastructure Services include:

Managed Services

Transfer the day-to-day management of your technology to us.

Virtualization

Make the move to a more dynamic infrastructure through Virtualization. Let Velocity show you how.

Security

Protect your network from the online threats that could literally put you out of business before it´s too late.

We have been in business in Asia since 1998.

Our team is made up of expatriates from Canada and Australia and the best local talent in Hong Kong and Manila.

We're small enough to care: Flexible and familiar.

We're big enough to be effective: With a management team who have either worked in Fortune 500 companies or advised local listed companies, but have the desire and drive to go out on our own.

Benefit from sensible approach to IT: Common sense and a clear view of what works and what doesn't.

Other Services & Solutions

- Cloud Solutions
- Business Analytics
- Mobile Applications
- Disaster Recovery and Business Continuity
- Hosted Solutions
- IT Consulting & Implementation
- Software Architecture & Development
- Offshore Software Development and Support

1802 Wan Chai Commercial Centre
194 Johnston Road
Wan Chai, Hong Kong

Phone: +852 2915 5096
Fax: +852 2834 8852

www.velocity-technology.com