All the latest technology trends and topical issues

ISSUE 4 - 2016

technology times

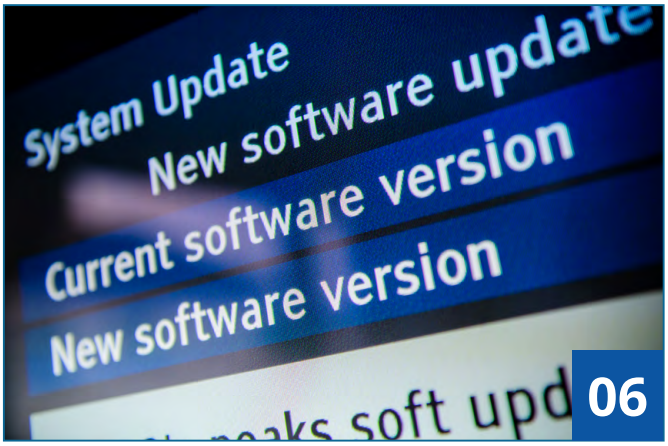
5 Ways to Spot A Social Engineering Attack

Missing Just One of These Could Instantly Open Up Your Computer Network to a Cyber Attack

Warning Signs your Computer is Infected with SPYWARE

Velocity Technology

Contents Issue 4- 2016



3 Stuart's Corner
Magazine Contact

4 5 Ways To Spot A Social Engineering Attack

5 Relying On A Good Luck Charm?

6 Missing Just One of These Could Instantly Open Up Your Computer Network to a Cyber Attack

7 Warning Signs your Computer is Infected with Spyware

8-9 CYBERSECURITY EVENTS

Anatomy of the Hack
Nomura Prime Expert Series
AustCham Business Technology Event
Cybersecurity & Compliance Seminar

10 Security Products

11 Free 1 Hour IT Review
Comics
Business Humour

Win HK$200 ParknShop Gift Voucher

HK Newsletter Team

Stuart Sanders
EDITOR

Michael Early
EDITOR IN CHIEF

Cristina Caratao
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!"

It's been a busy summer. I've been doing cybersecurity presentations both here in Hong Kong and regionally. Events included a round table for select HSBC Prime Finance fund clients, the inaugural Nomura Prime Finance Bento-Box luncheon, a joint Microsoft / FINEX event in Manila and various other compliance and Chamber of Commerce events.

In many ways, 2016 has been a watershed moment for cyber security. While it's not a new issue, it has certainly hit mainstream news and the imagination of the public at large. A fair amount of the news this year is old news in some ways. Some of the more public breaches (LinkedIn and Facebook for example) actually occurred in 2012 but have only recently become publicly known about. The criminals behind the hacks no longer had a use for data that was 4 years old and sold it to anyone willing to pay a few hundred dollars. As anyone who has been to one of my presentations will have heard, I believe the current state of affairs will not improve in the near term. The rewards for successful cybercrime are massive and the cross-border nature of it means that prosecutions are mostly rare.

The current situation is also hampered by a shortage of experienced professionals in the cybersecurity industry. Cybersecurity spending will continue to need to increase and move beyond just spending on firewalls and antivirus. If this is an area you are feeling challenged on, feel free to contact me and we can show you some affordable ways to dramatically increase your preparedness.

As always. Stay safe online until next time.

STUART SANDERS
Managing Director
Velocity Technology

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

5 Ways to Spot A Social Engineering Attack

"I'm not going to make payroll – we're going to close our doors as a result of the fraud."

Unfortunately, that statement is becoming more common among smaller businesses, according to Mitchell Thompson, head of an FBI financial cybercrimes task force in New York.

The FBI reports that since October 2013 more than 12,000 businesses worldwide have been targeted by social engineering–type cyberscams, netting criminals well over $2 billion. And those are just the reported cases. Often, due to customer relationships, PR or other concerns, incidents go unreported.

These unfortunate events were triggered by a particularly nasty form of cyberattack known as "social engineering."

Social engineering is a method cyber con artists use to lure well-meaning individuals into breaking normal security procedures. They appeal to vanity, authority or greed to exploit their victims. Even a simple willingness to help can be used to extract sensitive data. An attacker might pose as a co-worker with an urgent problem that requires otherwise off-limits network resources, for example.

They can be devastatingly effective, and outrageously difficult to defend against. The key to shielding your network from this threat is a keen, ongoing awareness throughout your organization. To nip one of these scams in the bud, every member of your team must remain alert to these five telltale tactics:

1. **Baiting** – In baiting, the attacker dangles something enticing to move his victim to action. It could be a movie or music download. Or something like a USB flash drive with company logo, labeled "Executive Salary Summary 2016 Q1," left where a victim can easily find it. Once these files are downloaded, or the USB drive is plugged in, the person's or company's computer is infected, providing a point of access for the criminal.

2. **Phishing** – Phishing employs a fake e-mail, chat or website that appears legit. It may convey a message from a bank or other well-known entity asking to "verify" login information. Another ploy is a hacker conveying a well-disguised message claiming you are the "winner" of some prize, along with a request for banking information. Others even appear to be a plea from some charity following a natural disaster. And, unfortunately for the naive, these schemes can be insidiously effective.

3. **Pretexting** – Pretexting is the human version of phishing, where someone impersonates a trusted individual or authority figure to gain access to login details. It could be a fake IT support person supposedly needing to do maintenance...or an investigator performing a company audit. Other trusted roles might include police officer, tax authority or even custodial personnel, faking an identity to break into your network.

4. **Quid Pro Quo** – A con artist may offer to swap some nifty little goody for information... It could be a t-shirt, or access to an online game or service in exchange for login credentials. Or it could be a researcher asking for your password as part of an experiment with a $100 reward for completion. If it seems fishy, or just a little too good to be true, proceed with extreme caution, or just exit out.

5. **Tailgating** – When somebody follows you into a restricted area, physical or online, you may be dealing with a tailgater. For instance, a legit-looking person may ask you to hold open the door behind you because they forgot their company RFID card. Or someone asks to borrow your laptop or computer to perform a simple task, when in reality they are installing malware. The problem with social engineering attacks is you can't easily protect your network against them with a simple software or hardware fix. Your whole organization needs to be trained, alert and vigilant against this kind of incursion.

Relying On A Good Luck Charm?

Carrying a four-leaf clover might work for leprechauns. But when it comes to Internet abuse by employees, you're going to need more than sheer luck.....

Did you know?

- 70% of all web traffic to Internet pornography sites occurs during the work hours of 9 a.m. – 5 p.m.
- Non-work-related Internet surfing results in up to a 40% loss in productivity each year at American businesses.
- According to a survey by International Data Corp (IDC), 30% to 40% of Internet access is spent on non-work-related browsing, and a staggering 60% of all online purchases are made during working hours.

The list goes on, and the costs to your company can be staggering.

What types of web sites present the greatest risk? Categories include abortion, alcohol, dating, death/gore, drugs, gambling, lingerie/swimsuits, mature, nudity, pornography, profanity, proxy, suicide, tobacco and weapons.

Risks these types of websites expose your business to malware, viruses, fraud, violence, lawsuits, loss of confidential or proprietary data and more. Even social sites, while perhaps not quite as risky, can have a major impact on productivity.

Barriers that once stood at the edges of your office network have been annihilated by digital media.

Web content filtering is now crucial to network security – not to mention employee productivity – in this emerging environment. It can be deployed in a number of ways, but basically they boil down to two: inline and endpoint filtering.

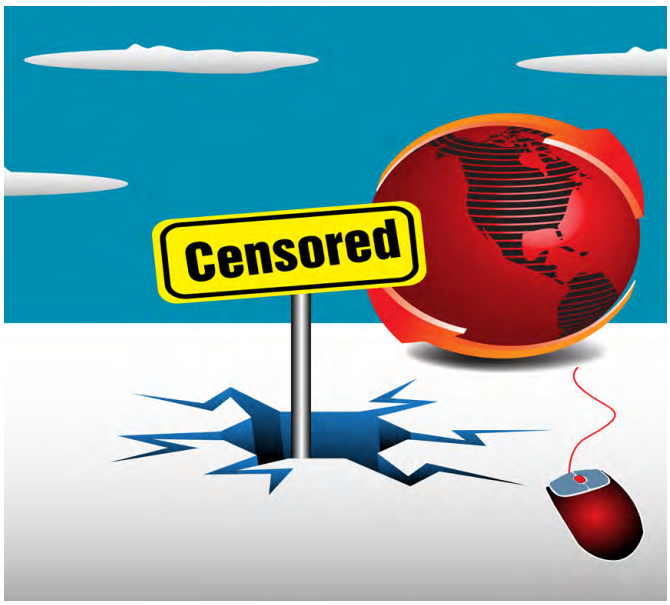
Inline Web Filtering

One way to filter web content is to control it at the entry point or gateway to your network. This technique intercepts all web traffic and applies filters that allow or block web access requests. Because the entire network is filtered, no access to the user's device is required.

With inline web filtering, there's no need to expend resources managing content at each endpoint – your employees and their computers, whether desktop or mobile. Inline filtering not only saves bandwidth, it goes a long way toward mitigating cyberthreats. For securing activities that take place within your network, it's a critical and potent strategy.

Yet, with the shift away from traditional office-bound work routines to a work-from-anywhere culture, the effectiveness of inline filtering has diminished. When employees access the web outside your network's gateways – via home networks, hotels, coffee shops, etc. – their devices become vulnerable to attack.

And any employee can carry an infected machine into and out of your company's building and network on any given day, exposing your entire intranet to infections. And that's why so many companies are moving to endpoint-based web filtering to complement their inline filtering.



Endpoint-Based Web Filtering

Endpoint-based filtering protects employee devices from infections, no matter where they connect to the web. Software at the endpoint – your employee's device – carries a predefined filtering policy from the central server that can be intranet-based or cloud-based.

The endpoint filter is then updated periodically from your company network. This method assures that web filtering is always active, no matter which gateway the machine connects through. The downside is that it must be rolled out and maintained at all endpoints.

That being said, one advantage of endpoint-based filtering is that it addresses stringent employee privacy regulations that are quickly becoming the norm in Europe and elsewhere around the world.

Because it keeps browsing-pattern information within the user's device, endpoint-based filtering provides a fairly non-intrusive way to handle employee privacy concerns.

And finally, while endpoint-based filtering really is the only way to protect a network without boundaries, as most companies now have, ideally it works hand in glove with inline filtering.

Because it keeps browsing-pattern information within the user's device, endpoint-based filtering provides a fairly non-intrusive way to handle employee privacy concerns.

And finally, while endpoint-based filtering really is the only way to protect a network without boundaries, as most companies now have, ideally it works hand in glove with inline filtering.

Forget the Charms – You Can Bet On This

We highly recommend rolling out not only inline and endpoint filtering, but also an effective training program for your staff to encourage best practices and assure compliance with your company's web security policies and procedures.

Missing Just One of These Could Instantly Open Up Your Computer Network to a Cyber Attack

WELCOME to the brave new world of cyber-warfare. Gone are the days when software patches were just for nifty little feature add-ons or updates.

Today, a software update notice could mean your whole computer network is suddenly at risk. Dangers include data theft, crippling malware attacks and mischief you may not discover for months, or even years...

As with graffiti on your garage door, if you don't pay attention and clamp down on bad behavior, your problems have likely just begun...

And, like those who hire a professional security firm to keep thieves out of the warehouse, thousands of CEOs and business owners are now waking up to the fact that it's absolutely imperative to hire a pro when it comes to securing your data network.

Here's why you need a professional handling this for you:

1 Speed is of the essence.

"If you didn't update to version 7.32 within seven hours, you should assume you've been hacked." That's what software maker Drupal told millions of its customers around the world last year. It's just one example of what can happen if you don't respond with lightning speed.

Once a security breach has been identified, hackers rush in. On "Day Zero," cyber-crooks around the world go after at-risk targets. You've got to be quick to patch the gap, or else you risk a system compromise.

Unless you have the time, knowledge, experience and tool set to respond instantly, you are far better off leaving this to a professional IT firm you can trust.

2 It's not just the big boys they're after..

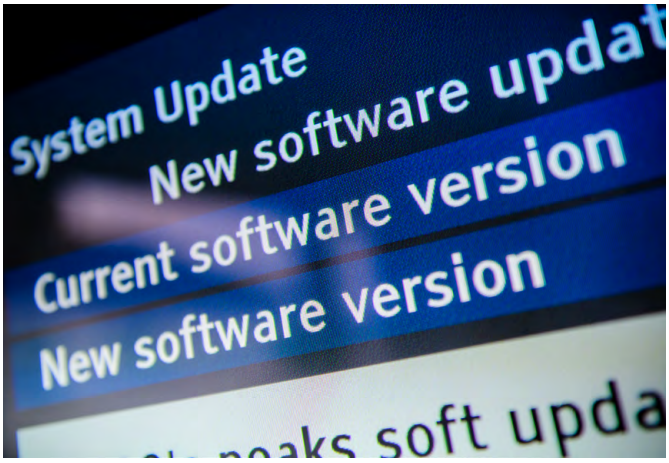
Sure, the top news stories are about the attacks on companies like Target, Home Depot and Sony... Yet your business is just as vulnerable, if not more so.

Chances are, you simply do not have the resources that giant corporations have to manage a data disaster. The statistics bearing this out are shocking: more than 60% of small businesses close their doors following a serious data breach.

The threat is not confined to giant corporations. Small and medium businesses are being attacked every day, and, unfortunately, your business is no exception.

3 Dealing with data breaches requires specialized knowledge, skill and experience.

Here are just a few of the things a competent data guardian must be able to do to effectively protect your systems:



Review documentation and monitor forums
Sometimes your software vendor doesn't tell the whole story. It's critical to check online forums and other communities to see if anyone else is having issues with the new patch before jumping in with both feet.

Know when to apply a patch immediately and when to wait
Typically, somewhere around 95% of patches work hassle-free. The trick is to spot the 5% that don't — before installing them. This requires identifying unique patching requirements and applying exceptions accordingly. For instance:

- *Does the patch deal only with a security issue*?
  Or does it just add new features or fix non-security-related bugs? Obviously, security issues get top priority.

- *Is the system currently having issues?*
  If not, and if the patch doesn't address a security issue your system is vulnerable to, it may be better to heed the old adage "If it ain't broke, don't fix it."

- *What security gaps does it address?*
  How severe is the threat to your particular network? If, for example, the only way a virus can enter your system is through an e-mail attachment and this functionality has been disabled for all users, perhaps the threat needn't be a great concern.

Keep options open in case of complications
Once a patch has been applied, if things aren't working, it's critical to restore the data network to pre-patch functionality, with little if any downtime. That means having good backups in place along with a tested and proven recovery process. Does just thinking about data security give you a headache? We strongly advise that you let us handle this critical part of your business for you.

Warning Signs

Your Computer Is Infected With Spyware

SPYWARE is Internet jargon for hidden programs that advertisers and criminals install on your PC without your permission to spy on you, gather information, and either report this information to a 3rd party for money or for identity theft and other criminal enterprises. Spyware might seem old hat, after all it has been around for a while, and as an attack vector has been superseded in popularity by crypto-ransomware, but it continues to be a threat. So we've considered it time to remind our readers about this.

Spyware is NOT harmless; traditionally it has been responsible for delivering a boatload of spam, altering your web browser, slowing down your PC, and serving up a bounty of pop-up ads. More recently though, it can be used for identity theft and to gain man-in-the-middle access to banking websites, log passwords and account details and use your PC for bitcoin mining and perhaps even illegal activities.

Most of this kind of malware finds its way onto your computer via file downloads including free programs, music files, and screen savers found everywhere on the Internet. These nasty programs piggyback the download and run undetected on your computer. Although spyware has malicious components, it is not illegal as you agree to the terms when you download and install what might seem like useful free software, and it is not considered a virus because it doesn't replicate itself or destroy data.

If you are experiencing one or more of these warning signs, chances are your computer is infected and you may need to seek professional help in getting the spyware removed, or simply backup your files and do a factory restore.

1. **Your browser has been hijacked.** If you open your Internet browser and a strange-looking homepage pops up and won't go away, chances are you have a spyware program installed on your computer. You may also discover that you cannot modify your browser settings and that your favorite's folder has been modified.

2. **You conduct a search but another (unauthorized) browser completes it for you**. For example, you type a search term into Microsoft IE but another browser pops up and lists various websites tied to your search term. This is a surefire sign of a spyware infection. You'll also notice that if you try and remove this program, it comes right back.

3. **Your computer is unstable, sluggish, locks up, or crashes frequently.** Spyware programs run in the background taking up disk space and processor speed which will cause serious performance problems. Your computer could also be part of a network cracking passwords or mining cryptocurrency like bitcoin.

4. **You constantly get pop-up ads displayed on your screen, even if you aren't browsing the Internet.** Some of the ads may even be personalized with your name.

5. **Mysterious files suddenly start appearing on your computer, your files are moved or deleted, or the icons on your desktop and toolbars are blank or missing.**

6. **You find e-mails in your "Sent Items" folder that you didn't send.**

7. **Sites you normally use for https (secure browsing) are showing as unencrypted or unsafe.**

Even in 2016 spyware is prevalent on the Internet, it's particularly common to have extra things added with software hosted on popular download sites like download.com or cnet.com. There have also been recent examples of spyware being pre-installed on popular computer brands. Lenovo's home PCs were one example, which were pre-installed with Superfish in 2015 and caused a big media frenzy. Most spyware programs are designed to run undetected by the user. That means you could be infected and not even know it.

ANATOMY OF THE HACK - From Banking to Elections

15 June 2016 | Dusit Thani Manila, Philippines

Financial Executive of the Philippines (FINEX) and Microsoft jointly hosted a seminar entitled Anatomy of the Hack - From banking to elections.

Stuart Sanders was invited to speak along with other speakers including Eric Lam from Microsoft (Director, Microsoft Asia Enterprise Cyber Security Group), Warren Bituin from EY (Partner) and Anton Mauricio from CISI (Country President of Chartered Institute of Securities and Investments).

The event wrapped up with some insightful questions in the panel discussion at the end.

NOMURA PRIME EXPERT SERIES

You are "Under Attack" – Cyber Security For Asset Managers

17 June 2016 | Two International Finance Centre, Central, Hong Kong

Stuart Sanders was invited to speak at Nomura Prime Expert Series. He briefed the audience on current cybersecurity trends and threats and discussed some strategies around training and process that should be implemented.

The event attended by Asset Managers.

Cybersecurity risks and how to protect your business

Presented by AustCham Business Technology Committee Event

5 July 2016 | Commonwealth Bank of Australia Innovation Lab, Central, Hong Kong

In today's highly interconnected world, cybersecurity poses a genuine threat to businesses both large and small. Two key cyber risks are ransomware and identity theft are now an everyday corporate threat. Companies are now facing increasingly sophisticated threats from within their own organizations. This forum provided insight and specific advice on what businesses can do to protect their business from these and other forms of cyber-attacks.

This forum discussed what is trending in cybersecurity both globally and locally while advising on the business risks that this trend may pose.

The panel of experts provided guidance on whether you are doing enough to protect your business for today as well as safeguarding for the future.

CYBERSECURITY AND COMPLIANCE SEMINAR

29 June 2016 | Canadian Chamber of Commerce, Central, Hong Kong

Last June, Velocity Technology Limited together with Complyport (HK) Limited held its first CyberSecurity and Compliance seminar. It was attended by COOs and Managing Directors of Asset Management Companies in Hong Kong. The briefings covered the following topics: a brief evolution of digital threats and how money has changed the landscape; digital threats in 2016 including crypto-ransomware, CEO phishing fraud, and zero-day exploits; investors and regulators increasing interest in cyber-security; and some practical tips for defending your business.

The event speakers were Stuart Sanders of Velocity Technology Limited and Stuart Somer of Complyport (HK) Limited.

SECURITY PRODUCTS

Webroot SecureAnywhere Business Endpoint Protection focuses on delivering a high-performance endpoint malware prevention and management solution. It offers a highly accurate and effective endpoint malware prevention with a range of additional security shield capabilities that keep both the user and the device safe.

Webroot SecureAnywhere solutions use cloud-based management and offer a standard console or Global Site Manager console. All Webroot SecureAnywhere solutions are powered by the Webroot BrightCloud® Threat Intelligent Platform - the most powerful real-time threat analysis engine in the world.

Webroot SecureAnywhere key security features: Identity & Privacy Shield, Infrared, Web Threat Shield, Intelligent Outbound Firewall, Powerful Heuristics, Offline Protection, Virtualization, Terminal Server & Citrix Support, Mobile Smartphone and Tablet Support and Resilient Distributed Cloud Architecture.

http://www.webroot.com/us/en/business/smb/endpoint-protection

Dashlane is the world's best password manager and secure digital wallet that features an easy-to-use interface and an optional cloud syncing capability. Dashlane saves and stores passwords as you log into websites. It has a password generator that rates every password's strength and provides several options for new passwords. Dashlane has excellent auto-login and auto-fill features. As a digital wallet, it securely stores any and all payment types such as credit cards, debit cards, bank info and Paypal. It also automatically saves receipts and screenshots of user purchases.

Furthermore, Dashlane has a dashboard dedicated to security that scores the overall safety of user account. Dashlane is encrypted & secured with a Master Password and a Google Authenticator. The app is available on Mac, PC, iOS and Android.

https://www.dashlane.com/

EventLog Analyzer is an IT Compliance & Event Log Management Software for Security Information and Event Management (SIEM). It provides both agent-based and agentless SIEM software. EventLog Analyzer software helps monitor file integrity, conduct log forensics analysis, monitor privileged users and comply to different compliance regulatory bodies by intelligently analyzing your logs and instantly generating a variety of reports like user activity reports, historical trend reports, and more. This help mitigates sophisticated cyber-attacks, identify the root cause of security incident and prevent data breaches. It manages logs from distributed environment and monitors Windows, Unix and CISCO Events.

https://www.manageengine.com/products/eventlog/

ExpressVPN is a Virtual Private Network service that offers an unlimited bandwidth, top of the range encryption technology and access to numerous servers located all around the world. With more than 136 VPN server locations in 87 countries. ExpressVPN supports multiple protocols (SSTP, PPTP, L2TP/IPSec and OpenVPN) making it flexible and versatile for every tasks and activity that you require. ExpressVPN's network is SSL secured with 256-bit encryption. It supports Windows, Mac, Android, and iOS.

https://www.expressvpn.com/

Kaspersky Internet Security for Android gives you a wide range of tools to combat modern mobile malware & Internet threats. Kaspersky Internet Security protects user privacy, and safeguard personal data, even if the device is lost or stolen. Kaspersky Internet Security offers Android users top-tier malware protection, immediate response to the latest threats, protection from phishing attempts, anti-theft capabilities, remote control of lost or stolen device and simplified online management.

http://www.kaspersky.com/android-security

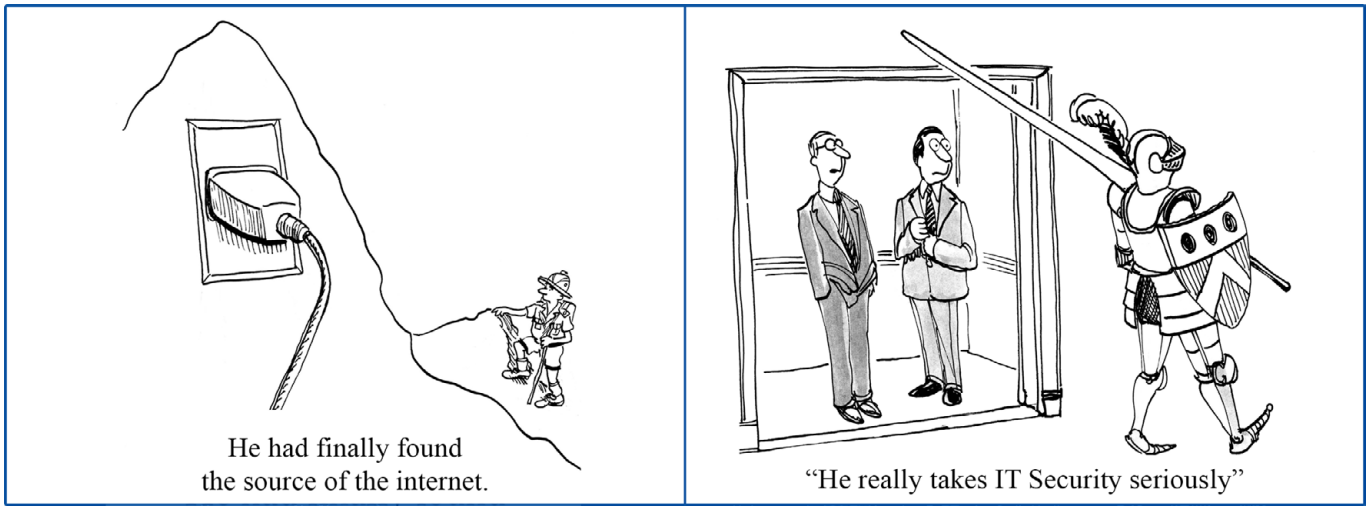
FREE 1 Hour IT Review for Your Business

Velocity Technology can provide qualifying businesses with a free 1 hour initial consultation to assess your current IT systems. We can examine your current IT systems and highlight any areas that could affect your business continuity or the productivity of your staff.

This is the perfect time to evaluate the state of your IT systems and position your company for increased efficiency and effectiveness in 2016!

Contact us today by emailing: **itreview@velocity-technology.com**

Or call us on **+852 2915 5096**



How Balloons Teach Teamwork

Once, in a seminar of about 50 people, the speaker decided to change his presentation to prove a point. He decided to do a group activity. He gave each person a balloon and asked them to write their names on it with a marker.

All the balloons were gathered up and put into a small room. The attendees were all let into the balloon-filled room and were asked to find the balloon with their own name on it within 5 minutes. As expected, everyone was frantically searching for their name, colliding with each other, pushing around others and creating utter chaos.

At the end of the 5 minutes, no one had found their own balloon.

The presenter then asked the attendees to randomly pick up one balloon and give it to the person whose name was written on it. Within minutes, everyone had their own balloon.

"This is what is happening in our lives," the presenter explained. "Everyone is looking frantically for their own happiness, not knowing where it is."

Our happiness lies in the happiness of others. Give happiness to other people, and you shall find your own.

This is the purpose of human life.

Have a Chance to Win a HK$200 ParknShop Gift Voucher

For this issue of the newsletter we will give away a HK$200 ParknShop Gift Voucher to the first correct email sent to **trivia@velocity-technology.com**.

The question for this issue is: **What is the name of the first Chief Executive of 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