POLICING The Pixels

Your Local Experts Tips for Cyber Security Week

ADVERTORIAL

security@clickstartit

Switched On Advice Cyber Security Sessions

Cyber Security Awareness
Wednesday 29th May 7pm - 8pm
Discover what cyber security is all about. We'll show you when you need security software and how to set it up properly.

Staying safe on Social Media
Wednesday 5th June 7pm - 8pm
Manage your privacy settings and friends lists on Social Media. We'll be talking about Facebook, Twitter and Pinterest.

Careful what you Click!
Wednesday 12th June 7pm - 8pm
Learn how to spot the difference between a legitimate message and a scam. We'll look at phone calls, emails, apps, links and more.

All sessions are FREE
Bookings preferred: Call 6964 1611 to secure your spot.
Clickstart IT :: lower block Banna Ave :: Griffith

clickstartit.com.au

What is National Cyber Safety Awareness Week?

THE internet has become part of daily life. We socialise, shop and do business online. Unfortunately, because we're sharing more personal information there, it also exposes us to greater risk of cyber crime.

National Cyber Security Awareness Week, May 20 to 24, is an Australian government initiative which aims to help Aussies using the internet, do so safely. There are simple steps that can be taken to protect your personal and financial information. Here are the top ten.

- Install and update security software and set it to scan regularly.
- Turn on automatic updates on all your software, particularly your operating system and applications.
- Use strong passwords and different passwords for different applications.
- Stop and think before clicking on links and attachments.
- Take care when buying online. Research the supplier and use a safe payment method.
- Only download applications from reputable publishers and read all permission requests.
- Regularly check your privacy settings on social networking sites.
- Stop and think before posting any photos or financial information online.
- Talk with your child about staying safe online, including on their smart phone or mobile device.
- Report or talk to someone if you feel uncomfortable or threatened online. Download the government's Cybersafety Help Button.

Clickstart IT

WANT to know more about how to be safe while online? Try one of Clickstart IT's upcoming information sessions.

First off the mark is Cyber Security Awareness on Wednesday, May 29 commencing at 7pm. Topics covered:

-Overview of Cyber Security and what it all means.
-What are the risk?
-Tips for keeping your computer safe from malicious software.
-What are the different types of internet security? How to choose.
-Installation and configuration of internet security software.
-Which devices need security software?

Next in line is Staying Safe on Social Media at 7pm on Wednesday, June 5.

Topics include:
-What is social media?
-Privacy settings on Facebook.
-How to edit your friends list.
-Privacy options on other social media platforms.
-How to spot a dodgy app or link.

Last, but not least, is Careful What You Click scheduled for 7pm on June 12.

Learn to tell the difference between legitimate and dodgy:
-Emails
-Messages
-Phone calls
-Applications
-Links
-Files

All sessions are free to attend, but bookings are preferred. Call 6964 1611 to book for any or all of the sessions or email info@clickstartit.com.au.

SWITCHED ON: Tegan & Aaron from Clickstart IT

Want to keep your business connectivity safe, secure and problem free?

Sole Australian Distributor of the
ENDIAN FIREWALL APPLIANCE

Imported from Europe
One stop solution for business network security
Unified Threat Management means safe and secure connectivity
Advanced functionality, simple interface

Veritech are your local networking and internet specialists, with over 18 years experience, specialising in solutions for small to medium businesses.

Veritech Corporation Pty Ltd

local.veritechcorp.com.au
(02) 6964 5377

Veritech

THERE are ups and downs to everything. The internet is no exception. While the internet has given us the ability to deal with more people, conduct more business, shop online and do research, it has also opened us up to certain threats.

Veritech's Livio Mazzon said that the risks were real, but they be managed with proper planning and tools.

"The people that are hackers are getting better at it," he said.

"They're now using social engineering techniques to coerce people into giving out their information.

"It's well known that there are well-organised criminal organisations collecting information all the time and they choose their time to use it to do the most damage."

Where you go, what you do on the internet is being monitored and collected all the time. Even Microsoft, Google and the Australian government collect data that way.

That becomes a problem when someone decides to target you.

There are plenty of risks online, especially these days, and it is getting harder and harder to know when you're at risk.

BUSINESS SOLUTIONS: Veritech's Livio Mazzon

Mr Mazzon said that the best thing to do was be aware when online.

"Think about the emails you open," he said.

"Some websites are dodgy. If they're not reputable you can usually tell."

Mr Mazzon also said that anti-virus was essential, no matter what device you are using.

"Some people think that you don't need anything on your mobile phone and that is probably true if you're talking viruses, but if you're talking about people trying to steal information from you, that's another thing all together," he said.

"There are people out there monitoring passwords. No matter what firewall you use, you're vulnerable."

The cost of protecting yourself online is not expensive when considered against the cost of loss of production. According to Mr Mazzon, a good security system can cost anywhere from $100 to $300 each year. He said it was like insurance.

Using common sense was Mr Mazzon's final recommendation when it came to protecting your online security.

"In real life, if you go down the street, you don't leave your purse on the stool behind you while you're eating lunch," he said.

"A lot of how to behave on the internet is common sense.

"If you walk down the street, you're vulnerable. You're vulnerable to theft, being sucked into something or led down a path.

"The threats are still there, they're just in more immediate vicinity.

"The internet increases the opportunity for threats from further afield."

Mr Mazzon said that businesses should have up-to-date firewalls, up-to-date end-device protection and common sense policy for internet usage.

POLICING The Pixels

Small Price for Peace of Mind

FOR parents of older kids and teens, the online sphere seems to be causing a fair amount of angst. Whilst the internet should be a tool that is both useful for schoolwork and just a bit of fun, there are some frightening stories that take the shine off its importance.

So what exactly is happening in the virtual world? Cyber-bullying is one serious problem that seems to be taking hold locally. Not only do bullies operate in the real world, they can now target their victims easily using social media.

Anthony Salmon from Flexible Solutions, a local firm specialising in proactive computer maintenance and security for both home and business, has seen first-hand the effects of this malicious bælity right here in Griffith. It's happening now and people are getting affected," explains Mr Salmon. "Parents need to be aware of these dangers. They should control and monitor their children's access to the internet."

Equally as important is the parent's need to protect themselves online. Confidential details, personal information, credit card details – these are all attractive targets for cyber-criminals' efforts.

"Whilst there is no absolute way to be 100% secure online, it's about reducing the probability to the lowest practical level," suggests Mr Salmon. "Spyware, malware, Trojans, viruses, hackers – with all these different types of threats, a multi-faceted approach that targets each risk individually is the most useful solution."

"People should have multiple tools and make sure they are up-to-date," warns Mr Salmon. "And it's important to check the reports they provide too. It's the best way to ensure everything is running smoothly and threats are being dealt with effectively."

Ensuring your online safety costs as little as $80 - $100 per year for home users. Businesses can expect to pay a similar amount. Money well spent when you consider the disruption to business if the network is down for a few days, not to mention the repair costs themselves.

Just one small, gold coin per week. Seems like a small price to pay for peace of mind.

Too Good to be True CYBER SCAMS

IF IT sounds too good to be true, it usually is. Cyber scams are everywhere and their aim is to get your money.

Watch out for:

-Unsolicited offers arriving by email or SMS.

-Enticing subjects with promises of lottery wins, wealth or weight loss.

-Emails using lots of capital letters, bad spelling, different fonts, unusual subject headings or with text appearing in images.

-Work-at-home schemes offering easy ways to make money.

-Incredible health claims for difficult-to-cure conditions and illnesses.

-"Phishing" emails claiming to be from a bank or other legitimate company asking for your account details (usually by providing a link to a fake login page).

-Lottery, sweepstakes or other prize wins, asking you to send money or personal details to claim your winnings.

-"Nigerian scams" asking for money or assistance to release a small fortune from a distant country and promising a share of the fortune in return.

-Modem jacking – make sure "free" adult sites don't download internet diallers. You could end up with a huge phone bill.

Here are a few easy ways to protect yourself.

-If you're unsure about the sender, delete the message. Do not reply or try to unsubscribe to the email or SMS. That will only confirm your address and you'll receive more spam.

-Never send your personal, credit card or online account details out in an email.

-Don't access banking and other online accounts from an email link – use a bookmarked link or type in the address.

-Always check the website carefully, scammers often set up fake websites with very similar addresses.

-Always read the terms and conditions carefully. Free offers often have hidden costs.

-Check the business name at www.asic.gov.au (Australian businesses only). You can also search for the business name or scheme through a search engine.

-Install software that protects your computer from viruses and unwanted programs and keep it up-to-date.

POLICING The Pixels

VIGILANT: Simon Mezzomo & Max Muravyov from Felxible Solutions keeping a watchful eye on client networks.

Five of the biggest IT hacks/attacks from history

1. Titan Rain - Hackers in southern China sat down at their computers in November of 2004 and set off on a hunt for U.S secrets. Since back in 2003, groups had been conducting assaults on U.S Governments in order to get their hands on sensitive information. This massive cyberspionage ring was codenamed "Titan Rain" by U.S. investigators. It was officially declared as a Chinese cyber attack on U.S. Security in 2005. Both U.S. military and defence contractors were breached by the attack.

2. Mafia Boy - In 2000, all it took was for a fifteen year old computer whiz to hack into several different commercial website and shutdown their system for hours. Among the websites affected were CNN, Yahoo, and EBay. Authorities only found out who was responsible after the boy bragged about it on a chat.

3. Sony Playstation Network - In late April of 2011, there was an outage which led to over 77 million users' personal information expose to the hackers. Sony lost about 2 billion dollars in damages and gained a lawsuit in the process of it. They were able to restore their network and offered free identity theft protection for users.

4. The Morris Worm - What seemed like a harmless experiment in 1988, turned out to be one of biggest accidents in history. Robert Morris created a worm across the internet which shutdown 10% of computers at the time. This raised awareness of internet and network security.

5. My Doom Virus - Nearly rendering emails useless and unreliable, MyDoom Virus attacked other computer by sending emails they breached from previously infected systems.

Common sense is key to fighting cybercrime

AFTER reading all the headlines about increases in cybercrime, it's quite amazing that anyone still turns on their computer. But according to local IT experts, the reality of protecting yourself from online hazards comes down to some simple tools and common sense.

But what actually is cybercrime and how does it affect the average person? According to Australian Federal Police, cybercrime is a catch-all phrase used to describe various threats in the virtual or online world. It includes serious nasties such as frauds and scams, and hacking, when criminals break in to your computer to steal personal information.

The purpose, of course, is financial. By poaching your details, these villains are able to steal your identity, access your bank accounts or launder money from other illegal activities. Often your information is shared with other criminals in their network too.

So, how do you protect yourself?

"If you want to participate in the online world, use common sense," advises James Scremin from Flexible Solutions, a local IT firm specialising in proactive maintenance and security.

"Some of the simplest things are most effective. For example, don't open emails from people you don't know. You wouldn't let a stranger walk around inside your home when you're not there, so don't allow them in to your life through your computer."

Emails promising untold wealth are also on the list of things to avoid.

"If an email pops up and offers you the possibility of winning lots of money from Nigeria, don't open that either," warns Mr Scremin.

"There are also a number of products you can buy to protect your computer when you're online. They are relatively cheap and generally very effective, and they certainly provide good value for money when you consider how much you have to lose," explains Mr Scremin.

Whilst there may be no 100 per cent guarantee of online safety, with common sense and simple tools, you can reduce your risks significantly and enjoy all the benefits that the internet has to offer.

National Cyber Safety Awareness Week runs May 20 to 24