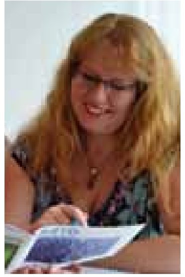
ISSN 1466-9358 online

MMIT
Multimedia Information & Technology

Volume 42 Number 3 August 2016

Combatting cybercrime ■ Marketing automation ■ Teaching information science in India

welcome



We are so pleased many of you are joining us in Sheffield in September for our two-day residential conference on digital citizenship and libraries, more details on page 3 of this issue. We will publish an overview for those of you who couldn't make it in person.

Warm regards,

Cathie

Catherine Dhanjal, Managing Editor

From time to time, MmIT offers space to suppliers who are developing and marketing products of potential interest to information services. Neither the journal nor the MMIT Group endorse any of the services covered in these pages. Articles published reflect the opinions of the authors and are not necessarily those of the editorial board or MMIT Group. While every reasonable effort is made to ensure that the contents of the articles, editorial and advertising are accurate, no responsibility can be accepted by the editorial board or MMIT Group for errors, misrepresentations or any resulting effects. Acceptance of an advertisement does not imply endorsement of the advertiser's product(s) by the editorial board or MMIT. ■

We'd love to hear your ideas for articles, reviews or case studies.

Just email the editor:

catherine.dhanjal@theansweruk.com

MmIT is published quarterly by the Multimedia Information & Technology Group of Cilip in electronic format in February, May, August and November. Copy deadlines: six weeks prior to publication. IP access or user name/password available. £75 p.a. for institutional subscribers.

For advertising, subscriptions and online access, contact:

Catherine Dhanjal
Managing Editor
Tel: + 44 (0)800 998 7990
or mobile: + 44 (0)7941 669925

Email:
catherine.dhanjal@theansweruk.com

04

09

14

24

26

contents

News

BFI news

Reviews

Features

Marketing insights

Technology roundup

and finally...

Cover image: https://pixabay.com/en/users/geralt-9301/

Will there always be cybercrime?

Kevin Curran is a Reader in Computer Science at the University of Ulster and group leader for the Ambient Intelligence Research Group. Ahead of speaking at the 2016 MmIT Conference he shares some tips for combatting cybercrime

Introduction

Greater philosophers than myself have pointed out that while we have rules and laws, humans come from different backgrounds and possess different morals. This means that society and the rules of the land will never comply so crime will always be in existence. Every person is different therefore those mind sets and the way they understand the law will be different. They may agree with each but the law does not comply with people's morals. We will therefore always have hackers.....and defenders. The cat and mouse game of patching vulnerabilities in systems and responding to data breeches looks like continuing for ever.

According to the National Crime Agency (NCA) Cyber Crime Assessment 2016 report cybercrime accounted for 53 percent of all crimes in 2015. This percentage is rising steadily each year. We can expect to see cybercrime continue to develop into a highly lucrative and well organised enterprise. Cyber criminals whether state sponsored or not are even beginning to devote funds to research and development! It has become an industry. We all remember the bank robber from 100 years ago who replied when asked why he robbed banks with the response "because that is where the money is...".

Well, criminals are increasingly moving online because that is where the money is. We are also seeing terrorist groups beginning to exploit cybercrime to fund their evil aims.

The latest demon online is ransomware. This is showing worrying trends. The Security vendor Malwarebytes used a 'honeypot' to attract attackers and they discovered an increase from 17% in 2015 to 259% in 2016. Ransomware of course is the nasty malware that holds peoples data files hostage until a payment is made in bitcoins.

Imagine the future however when our smart home devices are held hostage and owners have to pay a fee to have access to their lights and Internet of Things (IoT) appliances. We will also see ransomware appearing on our smart cars, trucks, trains and planes. It is only a matter of time before we see people left helpless, on the side of the road unable to drive their vehicles until they pay a ransom. Cryptocurrencies like Bitcoin of course have enabled the rise of ransomware.

In fact, experts predicts that by 2040 more crime will be committed by machines than by humans. This will arise as the human workforce moves towards more automation. What happens too when robots are hacked and change into suicide-bombing robots.

> ...we will also see ransomware appearing on our smart cars, trucks, trains and planes

The same applies to hijacking drones and perhaps using multitudes like flying bot armies to attack. We have already seen proof of concept WiFi hacking drones which can land on a roof and sit there intercepting WiFi, wireless keyboards and

other data being passed over a network.

It all comes down to practicing safe computing. What that is changes all the time. I list some good advice at the end of this article. Ultimately, trust no one. Encrypt all your data on the phone. Do not trust online cloud services like Dropbox. Encrypt it before it leaves your phone.

> ...we can expect to see cybercrime continue to develop into a highly lucrative and well organised enterprise

Don't trust email providers like Hotmail, Gmail, Yahoo etc. Use PGP (Pretty Good Privacy) to encrypt all your email messages.

Never trust public WiFi hotspots. Don't use torrent sites or illegal download sites. Do not use the phone for browsing.

Being paranoid is a virtue when you work in computer security.... It must always be remembered that no one involved in the early internet design ever foreseen the pervasiveness of its involvement in everyday life. That is why we have so many security & privacy issues today.

Here are some tips for practicing safe computing that I have collected:

- Keep software updated. Running the most recent versions of your mobile operating system, security software, apps and Web browsers is among the best defences against malware, viruses and other threats
- Use different passwords on all sites — and change them frequently
- Use a password manager
- Use an ad blocker — speeds up browsing and can protect against malware
- Keep your device secure by using a strong password to lock your smartphone or tablet
- Enable two-step authentication when offered e.g. Google
- When banking or shopping online, use only trusted websites that begin with https://
- Register with haveibeenpwned.com — and submit your email for future notifications
- Before downloading an app, make sure you understand

what information (i.e., location, your contacts, social networking profiles, etc.) the app looks for

- Do not download pirated or cracked software as it can often contain malware
- Do not click on popup windows that tell you that your computer is infected with a virus. Genuine antivirus software does not do this. The pop-ups install malware onto your computer, with your permission. Many now require you to pay money to have the software removed by the software originator. The new one called Cryptolocker is a nightmare. It is irremovable without paying a ransom
- Use antivirus software
- Whenever you buy an internet-connected device e.g. router, baby monitor, connected CCTV — change the default password
- Be careful with email attachments from unknown contacts
- Avoid using public wi-fi hotspots without using a VPN connection. A VPN will encrypt your communications to and from the internet to prevent eavesdropping
- Review your online accounts and credit report: you should review your bank accounts, auction accounts, and mobile phone accounts for signs of fraud or charges that you did not make
- Use touchID on iOS tablets & phones & register multiple fingers
- Lock down all internet traffic at home using OpenDNS. By filtering content at the router level, you can more easily control what you children access on their browsers
- To remain anonymous online — use the TOR browser
- Place tape over your webcam when not in use
- Use credit cards online. This protects you for purchases between £100 and £30,000. ■

Kevin can be contacted on Twitter: @drkevincurran or via email: kj.curran@ulster.ac.uk

coming soon...

November 2016

Features, including:

Advancing university learning through online platforms

Somme digital exhibition

News

Reviews

Marketing insight

Technology roundup

MMIT Conference 2016

September 2016, Sheffield, UK.
"The library's role in digital citizenship"
Find out more on the Group's blog: mmitblog.wordpress.com

Your articles, photographs, reviews, thoughts and suggestions for the journal are always welcome, just contact Catherine Dhanjal on catherine.dhanjal@theansweruk.com or call +44 (0)800 998 7990.

MmIT, 103 Bath Road, Willsbridge, Bristol, BS30 6ED, UK