Bits & Bytes

Volume 7 Number 6

In this issue:

Twitter

Facebook

Calendar

Dates to remember:

Training

Learn how to create and use a database when you attend the **Access 2013 Essential skills course** (3695). You will explore the Access environment, design, build and query a database, design forms and learn how to generate reports.

Don't store unlawful content

In the past year UCT received 18 take-down notifications from the Internet Service Providers Association (ISPA) for unlawful content on some of the machines on the university's network. As an ISPA member, UCT is bound by the ISPA Code of Conduct and has to meet certain standards in terms of privacy, consumer protection, spam and protection of minors.

Unlawful content can range from copyright infringement to illegally publishing an individual's personal information on a website. Any person or organisation can lodge a take-down notice to have unlawful content removed from the offending machine. Once ISPA has made sure that their requirements have been met, the offending member is sent a take-down notice requesting that the content is removed.

ICTS receives these take-down notifications on behalf of UCT and begins a process to locate and inform the offender (and the department or faculty in which they work or study) of the offence. From this point forward, the responsibility moves to that person's management team, who have to ensure that the offending content is removed and that the appropriate preventative and disciplinary action is taken.

Think before you click

Cyber-attacks are on the rise and hackers will stop at nothing to get access to your personal information. What's even worse is that universities are prime targets for hackers as they store large volumes of personal and research data.

Most attacks are caused by an individual either clicking a bogus link in an email or opening an infected attachment. These attachments often look like innocent Word or PDF documents, but once you click to open them, software is installed on your machine without you even knowing.

There have been a few incidents at UCT where a computer is infected with CryptoLocker, a ransomware Trojan that encrypts files and folders. These files can only be decrypted by the hacker once a ransom fee is paid before the given deadline.

In one case on campus, this malicious ransomware spread rapidly from the infected local drive (C:) to the UCT network, encrypting files in both cases. Files on the

See how effective Outlook can be as a productivity and time management tool at the **Outlook 2013: Effective email management course** (3464). The course comprises of ways to effectively use the Subject line, delivery and read receipts, conversation and reading pane features, folders, sort and filter functionality, rules and automatic replies.

If you are just getting started with Excel 2013 then our **Basics course** (3441) is ideal for you. The ICTS trainers will show you how to create, modify, format, print and manage worksheets. You will also learn how to perform calculations and how to set up a page.

If you already know the Excel basics, but are keen to learn more, then attend the **Excel Intermediate course** (3448). You will learn how to calculate data with advanced formulas, organise worksheet and table data, present data using charts and analyse data using Pivot tables and Pivot charts.

Be cyber safe and follow these handy tips

Personal information is like money. Value it. Protect it. Information about you, such as your purchase history or location, has value – just like

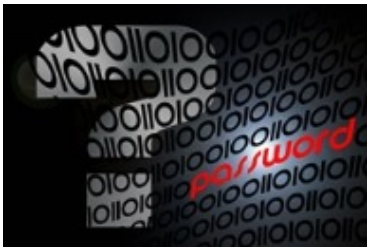
network drives were restored from backups, but none of the data from the C: drive could be recovered as the user had not done a recent backup. This resulted in the staff member losing valuable data.

If you think that your machine has been infected, don't try to open any files or folders. Immediately switch off your computer and remove the network cable from the back of your machine. Log a call with the IT Helpdesk by phoning x4500. The sooner you take action the better.

The McAfee EndPoint anti-virus will prevent certain behaviours of current ransomware from activating, but new strains are constantly being released. So rather be cautious and back up your data regularly. If you use an external hard drive, disconnect the device from your machine as soon as the backup is completed and store it in a safe place. Save all important university data on the network drives as these are regularly backed up.

Hackers rely on you being too busy or distracted and use you to deploy their arsenal. Don't be caught for a sucker – think before you click.

Passwords are your key to the network and you need to protect them



To protect the host of valuable information on the network, ICTS will no longer change passwords via phone or email. This means that you have to take responsibility for safeguarding your password. Here are some tips on how to do this.

- Update your contact information on Password Self-Service so that, if you forget your password, you can still get onto the tool to change it remotely via the web. A one-time pin (OTP) will be sent to either your mobile number or alternate email address. You can then access Password Self-Service and change your password.
- Don't use the same password for all your accounts and applications. If a hacker cracks the password, then you have thrown open the door to everything you hold dear.
- Keep your passwords secret and treat them the same way that you would your bank PIN.
- Don't write your passwords down and don't keep them in obvious places. Here are some very useful, secure password saving tools that you can use.
- Remember that, at UCT, if someone else logs on with your username, any action that they perform will be your responsibility as it will be your account details that were used.

money. Be thoughtful about who gets that information and how it's collected through apps and websites.

Share with care: Think before posting information about yourself and others online. Consider what a post reveals, who might see it and how it could be perceived now and in the future.

Be aware of what's being shared: Set the privacy and security settings on web services and devices to your comfort level for information sharing. It's OK to limit how and with whom you share information.

View our extensive security library that is brimming with tips and articles that will help you stay cybersafe.

Subscribe

Join our icts-newsletter-l mailing list.

Contact us

Email us your feedback, questions and comments.

By keeping your password safe, you are not only protecting your personal information, but also helping to secure valuable information on the UCT network.

Play your role in being UCT's first line of defence

You are UCT's first line of defence and need to be on your guard at all times to ensure that your information and that of the university cannot be affected by cyber-attacks. Always take the time to check an email before taking any action. Some of the tell-tale warning signs include checking the email address that you received the email from. Be wary of emails that you receive from unknown senders or domains. Check for spelling or grammar mistakes, as most people make an effort to check an email before clicking send. If you are required to click a link, first hover your mouse cursor over the link to check the URL. In most hacking cases these links go to a spoof website.

If an email looks suspicious, forward it immediately to UCT's Computer Security Incident Response Team (CSIRT). They will review the email and put the necessary precautionary measures in place to ensure that anyone who accidently clicks on the link is not affected. The team also has numerous monitoring systems in place to ensure that the UCT network and ICT services are secure. They are always on standby to handle any security breach no matter how big or small. So the sooner you report an incident the better. Early detection may prevent a bigger issue in the long run.

Getting to know cybersecurity lingo

Have you ever come across the term "trolling" while browsing the internet? Or what about "white hat" and "black hat"? These terms are becoming more commonly used now that people are taking more of an interest in cybersecurity.

We have compiled a short list of cybersecurity keywords that you may come across while browsing online:

Black Hat: A person who attempts to find computer security vulnerabilities and exploit them for personal financial gain or other malicious reasons.

White Hat: A computer security specialist who breaks into protected systems and networks to test and assess their security.

Critical Infrastructure: The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.

Cyberbullying: The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.

Data Breach: The unauthorised movement or disclosure of sensitive information to an authorised party.

Encryption: Converting data into a form that cannot be easily understood by unauthorised people.

Spoofing: The forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source.

Trolling: Making a deliberately offensive or provocative online posting with the aim of upsetting someone or eliciting an angry response from them.

University of Cape Town: Information and Communication Technology Services (ICTS) 7 Main Road, Mowbray, Cape Town 8000