# The Quarterly Newsletter of
# Information Technology

**Volume 1, March 2017**

**464 Monthly Users**

Are you part of this connected workplace?

## Chan Zuckerberg acquires Meta

"*Most scientific breakthroughs have been preceded by the invention of new tools that help us see and experiment in new ways.*" Mark Zuckerberg

Facebook CEO, Mark Zuckerberg, and Priscilla Chan's $45 billion philanthropy organisation has made its first acquisition in order to make it easier for scientists to search, read and tie together more than 26 million science research papers.

Meta is an Artificial Intelligence (AI) search engine and will be free to all later this year.

Meta will help scientists find the latest papers related to their own projects, and assist funding organisations to collaborate with researchers, identifying high poten-tial areas for investment or impact.

You can reserve an account now at www.meta.com if you would like to get early access to this capability.

## What's new in Information Services?

Kit Disney, our Information Services Business Relationship Manager. This role was created in the Information Services group to increase our engagement and collaborative planning activities with business partners all around UNE. Kit's focus is on the application needs of different UNE business areas, and brings a non-technical, business-level, strategic perspective to our team.

## From the Director

Welcome to the March edition of the IT newsletter. One thing that will be apparent is the amount of space we have dedicated to personal security in this edition of the newsletter. Whilst ITD invests significantly in IT security solutions, from the Sophos antivirus software running on your PC to next generation firewalls, there is always one significant risk and it is the largest we face—it's YOU and me, and every other human being that works, studies or interacts with UNE. All of the security in the world isn't going to stop a dedicated fraudster if we leave the bank vault door open, such as leaving our computer password written down in the top drawer of your desk. There are also countless different exploit attempts based on things such as social engineering. It's a confronting state of affairs that every one of us needs to take responsibility for security. We all need to become security savvy to protect ourselves and our colleagues. Please take the time to read the security messages in this newsletter, and participate in the online security training about to be released, it will save a lot of pain in the future!

In addition to this training, ITD has been running a Phishing campaign of its own through an external company. These test phishing emails test the maturity of our organisation to identify suspicious emails and how to respond (or not respond!) to them to protect ourselves. The number of UNE staff that have clicked on links and even gone on to enter their credentials is alarming, yet UNE is better than average, perhaps that comes with our online DNA, but we need to be much better!

Stepping down from my soap box, I'm pleased to advise that we have a range of new projects funded for 2017 that will see further improvement to the IT capabilities offered by UNE to staff, students and researchers. One significant project we have underway is the transition of our data centres to the public cloud; offering us a range of service improvements. The new identity management platform is progressing, which will again provide improved provisioning of services and capability to reset passwords. These are huge, multi-million dollar, multi-year projects but the benefits will be amazing.

In 2017, ITD is giving increased focus to improving staff satisfaction levels with ITD services. We are performing OK at 70%+ staff satisfaction rates, but we would like to see this move to around 75% satisfaction, which would very comfortably put us in the top 10 in Australia and New Zealand. We are focussing on our training, staff morale and business processes to achieve these improvements. If you have any feedback on what we can do to improve IT service levels please email or phone me, I would love to hear your ideas.

Finally, the new IT Strategy has been approved by the Vice Chancellor and sets the strategic direction of the IT teams at UNE for the coming three years. A copy of the strategy is available on the ITD website, and the focus is on supporting the University Strategy in the Digital World. How do we make our processes better for students, staff and researchers? How do we become the online university of choice? Because we are so easy to deal with and provide such a superior experience that students won't want to study anywhere else and staff or researchers won't want to work anywhere else?

*Enjoy the newsletter.*

Robert Irving
Director ITD

## Dealing with Social Posts

- Hover over hyperlinks in emails to see where they truly lead. Better yet, type a known URL into your browser. #Phishing #CyberAware

- "Verify your account by midnight or it will turn into a pumpkin!" Get a message urging you to take action? Delete it! #Phishing #CyberAware

- Afraid you've fallen for a #phishing scam? Stop what you're doing & change your password immediately! Then notify the Help Desk. #CyberAware

- Receive a suspicious e-mail from a friend or colleague? Call them to ask if they sent it. #Phishing #CyberAware

- Posting personal information publicly provides fuel for scam artists.

    #Phishing #CyberAware
    #PrivacyAware


**InPlace** Smart Placement Solutions

## InPlace update

ITD have been working closely with the School of Nursing's Clinical Office to implement the placement software system *InPlace*.

The use of *InPlace* at UNE was initiated by the School of Education in 2014 for their teaching placements and is currently used by a number of disciplines across campus.

The Nursing and Social Work staff were using a placement system called Sonia but had some issues with the system in 2016. In collaboration with ITD they have now moved onto InPlace. The team opened the system to students in February.

## Don't forget your backup!

If you haven't set up a **backup for your important data,** now is the time to do so.

"**Barney**", is UNE's Windows file storage, and one place that is available for keeping copies of your important files, but there are also a couple of cloud options worth looking at.

A tool called **OwnCloud** allows you to set up certain folders to **"sync"** automatically between your desktop and the cloud store.

For more information to go:

http://www.une.edu.au/staff-current/staff-services/it-services/server-space
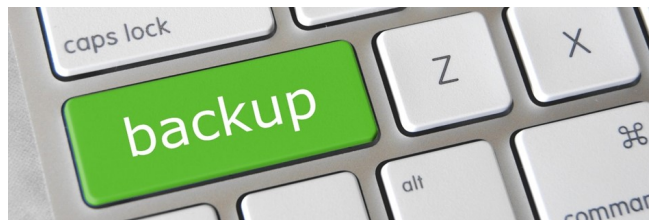


## Large print jobs?

If you have a large print job to run, it might be more cost effective to use the FujiXerox Document Centre on the ground floor of Building C034 rather than your local prrinter..

Your PrintCentre team at UNE are trained and dedicated to provide you with a superior and exclusive service that ensures important documents won't be compromised. Documents are printed using the latest in Fuji Xerox print technology, delivering outstanding document and finishing services that not only look professional, but make a real impact.

Using our PrintCentre couldn't be easier, simply send your request via email to **printroom@iinet.com.au** or call **02 6771 2420** for a representative to visit you or simply just drop into the PrintCentre.



## New fax gateway solution trial

The infrastructure team is in the middle of trialling the introduction of a new fax gateway system that will ultimately replace the discrete fax machine fleet currently in use around UNE.

Unlike standard email, the fax is still considered a legal document, necessitating their use in legal, financial, medical and regulatory environments.

The new solution integrates into UNE's Exchange environment, meaning that faxes can be sent and received via the user's preferred Outlook client, regardless of physical location.

The benefits include greater productivity, less paper use and reduced costs of administering and maintaining clunky old fax machines with mechanical parts that can break and jam.

## Learn what it takes to refuse the Phishing bait!

Cybercriminals know the best strategies for gaining access to your institution's sensitive data. In most cases, it doesn't involve them rappelling from a ceiling's skylight and deftly avoiding a laser detection system to hack into your servers; instead, they simply manipulate a community member.

According to IBM's 2014 Cyber Security Intelligence Index, human error is a factor in 95 percent of security incidents. Following are a few ways to identify various types of social engineering attacks and their tell-tale signs.

- Phishing isn't relegated to just email! Cybercriminals will also launch phishing attacks through phone calls, text messages, or other online messaging applications. Don't know the sender or caller? Seem too good to be true? It's probably a phishing attack.

- Know the signs. Does the email contain a vague salutation, spelling or grammatical errors, an urgent request, and/or an offer that seems impossibly good? Click that delete button.

- Verify the sender. Check the sender's email address to make sure it's legitimate. If it appears that the UNE Service Desk is asking you to click on a link to increase your mailbox quota, but the sender is……………… "*UniversityHelpDesk@yahoo.com,*" it's a phishing message.

- Don't be duped by aesthetics. Phishing emails often contain convincing logos, links to actual company websites, legitimate phone numbers and email signatures of actual employees. However, if the message is urging you to take action—especially action such as sending sensitive information, clicking on a link, or downloading an attachment—exercise caution and look for other tell-tale signs of phishing attacks.

- Never, ever share your password. Did we say never? Yup, we mean never. Your password is the key to your identity, your data, and your classmates' and colleagues' data. It is for your eyes only. UNE Service Desk will never ask you for your password.

- Avoid opening links and attachments from unknown senders. Don't open attachments unless you're expecting a file from someone. Give them a call if you are suspicious.

- When you're not sure, call to verify. Let's say you receive an email claiming to be from someone you know—a friend, colleague, or even the Vice Chancellor. Cybercriminals often spoof addresses to convince you, then request that you perform an action such as transfer funds or provide sensitive information. If something seems off about the email, call them at a known number to confirm the request.

- Don't be tempted by abandoned flash drives. Cybercriminals may leave flash drives lying around for victims to pick up and insert, thereby unknowingly installing malware on their computers. You might be tempted to insert a flash drive only to find out the rightful owner, but be wary—it could be a trap.

**Sources**:

The Awareness and Training Working Group of the EDUCAUSE Higher Education Information Security Council (HEISC).

STOP. THINK. CONNECT. When in Doubt poster.

## Identity and Access Management (IAM) project update

The project continues to deliver changes to the way that UNE digital identities are created and managed. These changes will enhance identity security and make management of your digital identity more efficient. Users of UNE systems and information will be able to personalise your experience by having more control over your identity information. An example of this control is the self-service password reset functions that will be released towards the middle of 2017.

Additional features due for release later this year will augment group and role-based access to make provisioning of your services and entitlements less manual and more transparent.

For more information contact: Tim Cross (Information Security Manager) and Ian Gesch (IAM Project Manager).

# From the Vault

### Network proxy/caching server (for Web, ftp and gopher requests)

Now that the University has a 2 Mbit/s link to the Internet and Telstra has a 24 Mbit/s link to the USA the speed at which you can access material from the World Wide Web and via "ftp", the file transfer protocol, is much improved. You can further improve your chance of getting better download speeds by utilising the "proxy and caching" server run by ITS.

After your Web client software, whether it be Netscape, Mosaic, Internet Explorer or whatever, has been configured to use this proxy server all Web requests made by you are first checked against cached pages already stored on the server. If the server has a recent copy of your requested page you'll get it straight away. If the server doesn't have a copy of the page you want it'll fetch it on your behalf, give it to your Web client and then store that page locally in the event that you, or someone else, asks for that page soon again.

The benefits are many. You may get better response times, the next person to ask for that page will definitely get a better response time and, over time, the University's Internet bill will be less that it might have been.

I don't have space to illustrate the details of configuring the proxy server into your particular Web client. Suffice to say that in "Netscape" it's in the "options | network preferences" menu, the hostname to add is proxy.une.edu.au on port 8080 and in case of difficulty contact the Help Desk on ext. 5000 or e-mail to helpdesk@metz.

**Trivia time: not so trivial**

There are several electronic mail servers on campus. The largest is "metz" with about 5000 e-mail accounts. Last week metz handled over 65,000 e-mail messages - local, domestic and international.

UNE has a modem pool on which 64 modems are currently configured. Over the past 7 weeks 638 individuals have connected to the campus network remotely. There were over 25,000 dialup sessions, 17,110 of these were PPP connections ("dial up Internet").

**Source:** ITD Newsletter From Vault/NetTalk/NetTalk-19960524

**In comparison:**

UNE now has a combined total of 40Gbps of internet and AARNet bandwidth – which is 1,500 times more bandwidth than back in 1996!!!

We now also have a centralised mail server system supporting over 5,000 user accounts, with unified voice, voicemail and email services, with all services available on your desktop computer, desktop phone or mobile device.