MEGA

BHS
Information
Technology

November 2016, Vol 3

CYBERSECURITY

Sitting at your computer, or using your smart phone it's easy to forget that your individual device is part of a network eco-system. The benefits of the Web have, of course, have come at some cost, including a loss of privacy. We are more vulnerable to data breaches and identity fraud. But there are many things we can do to minimise the risks of both.

Recently, Ballarat Health Services has fallen vulnerable to two different Phishing attacks, the first incident sent out '800 thousand' malicious emails whilst the other sent out '1.6 million'. Taking over 2 weeks to recover from, staff couldn't send or receive external emails impacting staff and patient care throughout BHS.

PHISHING

What is it? Often posing as a request for data from a trusted third party, phishing attacks are sent via email and ask users to click on a link and enter their personal details.

How does it work? Phishing emails include a link that directs the user to a dummy site. This site will then steal the user's information, in some cases, all a user has to do is click on the link.

How can I prevent it? Make a phone call to verify any requests from institutions that arrive via email. Most companies will not ask for personal information via email. At the same time, most companies strongly recommend that users not send sensitive information via email.

CASE STUDY ON SPEAR PHISHING

A Project Manager received an email containing a password protected file from whom they thought was from a familiar contractor. The email included the contractor's signature, was addressed to the project manager by name and contained details of relevant work projects. The sender's email address was a Gmail address created by the 'sender' that contained the contractor's full name. The email was forwarded for action with the 'sender' copied in and later triggered an alert and was blocked and sent to quarantine. The email contained a Windows screensaver file that would have appeared on the system as a PDF file. Once opened it would have dropped a malicious file that would have been used to monitor the behavior of the user containing details of the infected system.

DID YOU KNOW?

- Cyber-attacks in the healthcare industry are up 125% since 2010, and the likelihood of cyber-attacks in this particular industry is greater than any other sector in the economy (Infosec Institute, 2016)
- Cyber criminals raided the healthcare sector more than any other in 2015, with more than 100 million healthcare records being compromised (Infosec Institute, 2016).

COMPETITION TIME

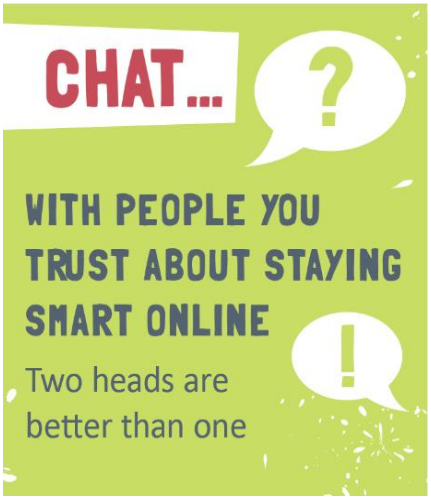
For your chance to win
2 x free movie tickets
simply email Jackie McLinden and tell us what you believe are some of the cyber security risks in your work area and how they can be resolved.
Entries close- 5pm 9th Dec. 2016

NEED HELP?

Staff can contact the
I.T Helpdesk between
800 – 1630, Mon – Fri on:
P: 5320 4786 ext. 94875 OR
E: HelpDesk@bhs.org.au

FEEL LIKE A FREE COFFEE?

'COFFEE with I.T' is an initiative designed to get you away from the office and provide you with the opportunity to discuss your ideas or potentially have the I.T department offer suggestions on improving work processes for yourselves or your department. Improving a work process could mean saving staff time therefore saving the department and BHS wasted expenditure that could be resourced elsewhere.



As the ICT Training and Support Officer and staff of IT we want to welcome suggestions and challenge staff to raise their ideas all over a '**free coffee'**. For bookings and further discussion please contact Jackie McLinden on ext. 98987.

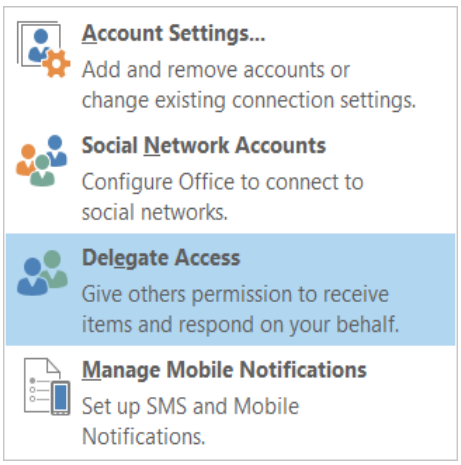
ARE YOU PLANNING ON LEAVE?

Are you planning on having leave over the Christmas period?

If you need temporary access user's files (e.g. if covering for someone on leave), where appropriate have your manager contact the IT helpdesk. They will be able to grant the access rights under your own ID, without compromising the ID of the person who is out of the office.

DID YOU KNOW?

If going on leave you can also delegate your Inbox, Calendar, Tasks, Contacts, and Notes. "Delegate Access" allows the people you nominate to see, edit or send items on your behalf
To delegate your email access- Click on FILE > INFO > ACCOUNT SETTINGS and select Delegate Access.



WHO IS RESPONSIBLE?

Securing our information cannot be ignored. It is the 'everyone's' responsibility. We now live in a connected world in which industry, government and consumers share the same communication channels. In essence, we are all in this together. In the health care system, one person's lack of responsibility not only harms that individual but provides a platform for other innocent users to be attached. It places a risk to staff and patients confidentiality as well as our integrity of our data.

DID YOU KNOW?

- There are over 3.6 Billion internet users – some of whom are maliciously motivated.
- Around 40% of the world population has an internet connection today;
- In 1995, less than 1% of the world population had the internet;
- In 2015, the average economic impact of cybercrime on Australian Organisations was $4.9 million;
- In 2015, the average time it took to resolve a cyber-attacked in Australian Organisations was 31 days.