IT SECURITY WEEK 2015

During IT Security week (26-30 January 2015), we posted a news item to our website each day that offered tips and guidance on the latest IT Security developments.

Is your password keeping your data safe?
The week kicked off with an article on secure passwords. For the second year in a row, ‘123456’ has topped the list of Worst Internet Passwords. Why should this matter to you; your password is secure, right? Your passwords protect your personal information and data.

Have a look at our article on the worst internet passwords and see if your passwords rank and what you can to do to create safe passwords.

Data Protection Day 2015
To mark international Data Protection Day on 28th January, there was an exciting panel discussion in the Synge Theatre - What does the internet say about you?

Held in conjunction with Information Compliance and the Science Gallery, this event was aimed at raising awareness and educating individuals on their rights and their responsibilities with regard to collecting, storing and processing personal information. The event also focused on encouraging businesses and other organisations to understand their responsibilities by being open and honest about how they collect, use and share personal information.

Think before you click!
An exercise in data protection - You may have noticed a giant QR code being projected onto the Nassau Street entrance to College? Over 100 people scanned the code and were asked a sequence of questions requesting personal data ranging from name, gender, email address to more sensitive data such as date of birth, occupa-
tion and credit card details.

Without any idea of what their information would be used for or where it was going to end up, 90% of participants volunteered their name and gender while a shocking 27% of participants answered the request for details of medical conditions and their credit card number.

While this exercise was for demonstrative purposes only, it could easily have had a more sinister agenda. The moral of the story - think before you click!

Visit our website for complete articles regarding IT Security Week 2015.

RESEARCH DATA MIGRATION SUCCESSFULLY COMPLETED

In December 2014, the HPRC team undertook an upgrade of the GPFS filesystem that is shared across several compute clusters. The old hardware had been commissioned in 2008 and had recently suffered some failures, leaving the service highly at risk of losing research data.

Leveraging the College’s investment in Infrastructure as a Service (IaaS), an additional 60 terabytes of storage was purchased and installed in the new VNX system. This storage was connected by fibre channel to the existing HPRC I/O servers to allow the migration of the data to occur.

One of the key features of GPFS is the ability to add and remove disks from the filesystem without interruption to service. Therefore the migration of the data could run in the background with no impact on users.

The upgrade was carried out as a three step process:

- Extend the filesystem by adding the new disks
- Migrate the data from the old to the new disks
- Remove the now empty old disks from the filesystem

It was agreed to undertake this large operation in the days before the Christmas holidays. Overnight between 22nd and 23rd December, approximately 11 terabytes of data was migrated with no issues. Therefore, just before leaving for the holidays the migration of the remaining 25 terabytes of data was initiated. With a little remote babysitting over the holiday period the migration was completed without data loss or downtime.

Now all critical research data on the HPRC clusters is housed on new equipment with warranties and support contracts in place. Overall the project saved College approximately €120k by saving on the purchase of a replacement standalone storage platform for the HPRC systems.

One of the key features of GPFS is the ability to add and remove disks from the filesystem without interruption to service. Therefore the migration of the data could run in the background with no impact on users.

The upgrade was carried out as a three step process:

- Extend the filesystem by adding the new disks
- Migrate the data from the old to the new disks
- Remove the now empty old disks from the filesystem

It was agreed to undertake this large operation in the days before the Christmas holidays. Overnight between 22nd and 23rd December, approximately 11 terabytes of data was migrated with no issues. Therefore, just before leaving for the holidays the migration of the remaining 25 terabytes of data was initiated. With a little remote babysitting over the holiday period the migration was completed without data loss or downtime.

Now all critical research data on the HPRC clusters is housed on new equipment with warranties and support contracts in place. Overall the project saved College approximately €120k by saving on the purchase of a replacement standalone storage platform for the HPRC systems.

SOFTWARE IN COLLEGE COMPUTER ROOMS

IS Services are in process of releasing a new software management facility, called Application Jukebox, in College computer and teaching rooms across campus.

This new facility will greatly improve the current service for requesting and distributing software on Windows PCs. Software can be added and removed as required, will provide a means for reporting software usage, and offer more efficient software and license management.

Independent to the standard software available in computer rooms, this new facility can assign ‘speciality’ applications to specific computers, rooms and/or students. This will offer great flexibility to academic staff when booking and time-tabling computer teaching rooms.

As well, it can host multiple versions of the same application in the event that a later or former version is needed.

DIGITAL REPOSITORY OF IRELAND

IS Services wish to congratulate the Digital Repository of Ireland on their three E-Government awards, for

* Open Source Technologies
* Promoting Ireland Overseas
* Overall Winner

Winners were announced by An Taoiseach, Enda Kenny, at an event in Dublin Castle on Thursday, 29th January 2015.

The technical delivery of DRI is managed by the High Performance Research Computing team in IS Services.

IS Services Enewsletter FEBRUARY 2015
UPDATE: COLLEGE MOBILITY PROJECT

Following on from the completion of the design stage, a public procurement tender was released to select a vendor to supply and build the new Wi-Fi network which will comprise about 2,000 high performance Wi-Fi access points and associated infrastructure. The successful vendor has been selected and the new build stage will commence subject to governance approval and contract.

What happens next ...
The vendor will require a four week lead time, after which the central resilient core of the new network will be commissioned and installed.

We will develop a build-out schedule for high priority areas, such as student residences without Wi-Fi, and the schedule will be made available to the relevant areas for approval.

We will make all efforts possible to avoid disruption due to these works during the revision and examinations period.

CLOUD COMPUTING POLICY

Cloud computing is a term used to describe IT offerings which can be purchased as a service and used across the internet. These services offer convenience and flexibility; however the processes involved in correctly procuring and evaluating cloud services can be complex and subject to legal, ethical and policy compliance requirements.

That is why to help meet the challenges of adopting this new technology IS Services have developed policy and guidelines to assist College in the selection and use of cloud services. The guidelines include a checklist to be used by anyone considering a cloud computing service for all or part of their official College work.

The checklist addresses the following:

- Stakeholder and institutional requirements - deals with the service and the implications of its use for the College.
- Vendor considerations - outlines issues to be considered in relation to the vendor offering the service.
- Data issues - deals with College data and the implications of its use, considers if the cloud solution justifies the risk of processing data off-site and the possible costs of security audits. For sensitive data a College hosted system may offer cost savings in the long term.
- Payments details
- Support arrangements
- Exit strategy - clarifies what happens when the cloud service ends.

So if you are already using, or are planning in the future to start using, a cloud computing solution then please review the Cloud Computing Policy and Guidelines.

STAFF PROFILE

HELEN O’HARA
Head of Management Services

Who are you and what do you do?

I am the Head of Management Services in IS Services. It is my job to manage the design, development, implementation, support and oversight of optimised business intelligence and integrated management information systems.

What’s the next big thing in IT?

Cloud Platform as a Service (PaaS) is particularly exciting for me in my current role as it is an enabler of rapid development of applications along with web services and databases that are integrated via common standards.

What’s your favourite film, music to listen to?

My all-time favourite film is Casablanca. I watch a variety of tv shows, a lot of which have forensic or hospital themes such as CSI Miami and Grey’s Anatomy.
Can you spot a phishing message?

Your inbox can be a dangerous place! Lurking among the countless work and study related emails are fraudulent ‘phishing’ emails waiting to catch you unawares and trick you into divulging your College network password, your personal information or the login details for your Internet Banking, Apple iTunes or PayPal accounts.

To stay safe you need to be alert to the possibility of scams and fraud in your inbox. Common examples of the type of phishing emails we regularly receive in College may attempt to induce you to:

• Act quickly to prevent an account from being deactivated
• Take part in a system upgrade or other IT action
• Cancel payment for an item which you have not purchased

To avoid these types of scams you need to be vigilant and cautious, always take your time and consider the validity of what you are being offered.

Make sure you can confirm the identity of the company or individual with whom you are engaged in a transaction. Never provide sensitive personal information by email or on unfamiliar websites.

What should I do when I receive a phishing email to my College email account?

Staff members who receive a spam/phishing email to their staff email account should report it so that similar email is blocked in future. Doing this helps reduce the overall amount of spam/phishing email being delivered to College email accounts, not just your own. To report an email as spam/phishing:

1. Save the spam/phishing email message – in Outlook this would mean opening the email to view it and then choosing File – Save As and saving it to your computer
2. Create a new, blank email message and attach the saved spam message to it
3. Copy and paste the original spam message subject line into the new message subject line
4. Send the new message to junk@office365.microsoft.com

What do I do if I think I have responded to a phishing email in College?

If you have replied to a phishing message or clicked on any links within the email body and entered your College username and password please immediately change your password and report this to the Helpdesk (+353 01 896 2000).

Finally remember...

IS Services will never ever ask for your username and password via email and you can confirm any communications from us with our website isservices.tcd.ie or the Helpdesk.