IT Services Department
Seirbhísí TF
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Fheabhsú Cáilíochta
Quality Enhancement
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh
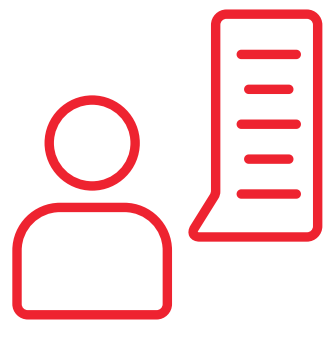
Case Study of Good Practice

Title: Securing UCC's data and information landscape
Presenter: Noelette Hurley, IT Services

Case Study Synopsis

In many ways UCC staff have all become content creators. Much of the content we create, policy documents, process information, support information has the potential to end up on our public website. As content creators it is our responsibility to recognise this and to consider how the information that we are collating and presenting to the public could be misused and to recognise that best practise determines that such information is identified that it needs to be made available is a secure way. The objective was to establish the idea that moving information that exposes UCC's practices and procedures off the public website and into SharePoint where it is secured behind our authentication processes as good practice.
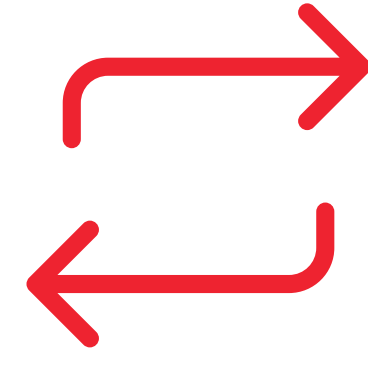
Intended Changes

- A targeted phishing attack is one where information around an individual and their reporting structures or work process is used to manipulate the individual into an action that costs them or their workplace money.
- One example would be impersonating a staff members line manager and requesting they purchase gift vouchers on their personal credit card for reimbursement later. Or on a larger scale manipulating our procurement processes to achieve a similar result but on a larger scale.
- Our objective is to work with departments to move such information to SharePoint where it can only be accessed with an official UCC account. Storing such information in SharePoint is good practise.

Key Impacts

- The establishment of a good practice that in turn increased security.
- Our sensitive information is protected by our authentication protocols, but still on a platform that relevant staff can access at any time, from anywhere.
- Additionally, overtime we will see a reduction in spear phishing attacks, as the information required to carry them out successfully will be much harder to come by.
- An unintended but welcomed outcome is an increased awareness around how seemingly innocuous information (such as who reports into who) can be misused to our detriment.
- In this case using SharePoint as good practice.

Additional Information

Many departments will have a legal requirement to share certain information around compliance with the public. It is therefore important to categorise the information and have a clear idea of the relevant audiences. Once it was identified what information needed to be moved SharePoint communication sites were planned and set up.

Planning a SharePoint site is as important as planning a public website. All sites need to have a clear purpose, audience, and communications plan. (This is another example of good practice).

Video Links | Graphics
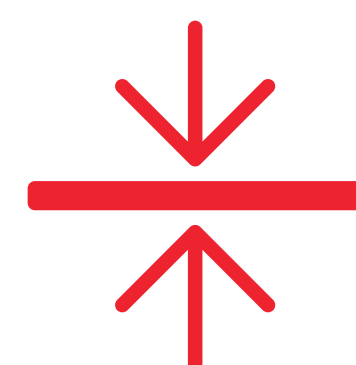
Area of Alignment

Infrastructure & Resources
People & Organisational Culture