University of Worcester

ICT Security Awareness

Reference code	ict-sec-v2
Author/originator	C. Austin
Review Date	1st October 2016
Ratified/authorised by	Zeb Amin
Issue date	22-01-14
Postholder/s responsible for review	Head of ICT

1. BEWARE of scams.
    - NEVER respond to an email asking you for your account details and NEVER disclose your password to anyone. The University or legitimate companies will never ask you to verify or provide confidential information in an unsolicited email.
    - ONLY click on links from trusted sources. Malicious email links can infect your computer or take you to web pages designed to steal your information. Never click on a mystery link unless you have a way to independently verify that it is safe.
    - DO NOT open unsolicited or unexpected attachments. Malicious attachments can infect your computer. If you cannot verify an attachment is legitimate, delete it.
    - DELETE all suspicious email immediately. Do not forward it to colleagues or ICT Support.

You should consider several factors when deciding whether an email is authentic.

- Look-and-feel: Be wary of emails which contain obvious spelling mistakes, poor grammar, or inferior graphics.
- Urgent action required: Be wary of emails containing phrases like "your account will be closed," "your account has been compromised," or "urgent action required." The fraudster is taking advantage of your concern to trick you into providing confidential information.
- Generic greeting: Fraudsters use automated programs to send thousands of malicious emails simultaneously. They may have your email address, but they seldom have your name. Be sceptical of an email sent with a generic greeting such as "Dear Customer" or "Dear Member."
- The sender's email address: Is it similar to, but not identical to a company's official email address? (e.g. *info@worrc.com* instead of *info@worc.ac.uk*) These email addresses are meant to fool you. In some cases fraudsters can forge the "From" address to look like a legitimate corporate address (e.g. @worc.ac.uk). Because of this, the "From" address is just one factor to consider when deciding if an email is trustworthy.
- Links to a fake web sites: Fraudsters often include a link to a fake web site that looks like the sign-in page of a legitimate web site. Just because a site includes a company's logo or looks like the real page doesn't mean it is!
- Masked links: Links that look like they go to the real web site, but don't. For example, the link text may say "University of Worcester ICT Support" but if you hover your mouse pointer over it you will see the link's real destination.

While some malicious email is obvious, others can be quite sophisticated and difficult to discern from the real thing, but to reiterate: ***The University and legitimate companies will never ask you to verify or provide confidential information in an unsolicited email.***

This advice should also be applied to texts, phone calls, Facebook, Twitter and all forms of Instant Messaging.

2. PROTECT information when using the Internet and email.
    - DO NOT log in to web sites unless the login page is secure. Look for ***https*** (not http) in the URL to indicate that there is a secure connection.
    - DO NOT send confidential information via email. Email is an inherently insecure method of communication.
    - BE CAREFUL about what you do over wireless networks. Information and passwords sent via standard, unencrypted wireless networks are especially easy for hackers to intercept. The University's **eduroam** and **UW_Secure** wireless networks are encrypted, but UW_Staff, UW_Guest and most public access wireless networks ARE NOT encrypted.
    - DO NOT share copyrighted files; this is illegal.

3. USE STRONG PASSWORDS that cannot be guessed or easily defeated by a computerised 'brute force' attack.

    - Effective passwords are those that display a lack of order or predictability (entropy), which are easy for humans to remember, but difficult for computer programs to defeat.
    - Historical ways of creating passwords by substituting numbers and symbols for letters are not effective in this respect i.e. they are difficult for humans to remember but easy for a computer to defeat.
    - An effective way to create a strong password that is easy to remember but difficult for a computer to crack is to use a string of words separated by spaces. This type of strong password is effectively illustrated here.
    - Test your current password using this Password Strength Calculator

4. USE TWO-FACTOR AUTHENTICATION on personal accounts.
    - Two-Factor Authentication (also known as 2FA or 2-Step Verification) adds a second level of authentication to an account login.
    - 2FA identifies an account owner by means of two different components, for example an account password PLUS a PIN code sent to the user's mobile phone.
    - You can enable 2FA on Apple, Amazon, Dropbox, Facebook, Google and Microsoft accounts, among others. Please refer to the individual accounts for more information.

5. DO NOT download or install unknown or unsolicited programs to your work computer.
    - These can harbour computer viruses or open a "back door" into your computer giving hackers access to your data without your knowledge.

6. SECURE your computer before leaving it unattended.
    - LOCK, LOG OFF, or SHUT DOWN your computer before leaving it unattended, and make sure it requires a secure password to start up or wake-up.
    - On a Windows PC use *<ctrl><alt><delete> or <Windows><L>*

- To lock a Mac select *System Preferences* from the Apple menu, then navigate to *Security & Privacy > General* and check *Require password immediately after sleep or screen saver begins.* You will then be able to lock your Mac using *<ctrl><shift><eject>*

7. ENSURE your computer is protected with anti-virus software.
    - Contact the ICT Service Desk immediately if you suspect your computer is infected with a virus.

8. SAVE YOUR IMPORTANT FILES on a network share such as the N or O drives, rather than to your local computer.

9. PROTECT portable and mobile devices.
    - DO NOT keep sensitive or confidential University information on portable or mobile devices, such as laptops, tablets, smart phones, memory sticks, CDs/DVDs, etc. unless they are properly password protected and/or encrypted. These items are vulnerable to theft or loss.

10. SECURE laptop computers and mobile devices at all times.
    - Use a Kensington lock to secure unattended laptops to a permanent fixture, or carry them with you at all times when out of the office. Contact ICT Support for advice on Kensington locks.
    - University provided mobile phones and tablets must be set with a PIN screen-lock.

11. SECURE your work area at the end of the day or before leaving it unattended.
    - Ensure you lock windows and doors, take keys out of drawers and doors, and never share your access card or keys.
    - Ensure you lock up portable equipment and sensitive material before you leave an area unattended.

I confirm that I have read and understand the good computing practices described in this document.

Signed: ____ Date: ____________________