Information security guidance documents

Information Technology (IT)

Guidance for University users on the most common threats to IT systems, services, and data.

1. Identity theft

1.1 What is it?

Identity theft is the process of stealing sensitive or personal information that is directly attributable to you e.g., date of birth, bank account/credit/debit card details, password credentials, home address, etc. that can then be used for malicious or criminally motivated purposes i.e., fraud.

1.2 How does it work?

A user is requested, prompted, or inadvertently ‘freely’ divulges information that can then be used to impersonate them or take actions on their behalf. This information can then be used to access University IT systems, open bank accounts, obtain legal documents (passports, birth certificates, etc.), make financial purchases, compose statements/libellous remarks in their name or in numerous other ways to cause distress, inconvenience, or financial harm.

1.3 Why is it so successful?

The benefits for obtaining personal or sensitive information can be far-reaching and may yield financial (or other types of) rewards relatively quickly with little risk of getting caught or suffering repercussions, and therefore these details are very attractive to attackers.

1.4 What steps can you take?

- Always be cautious and take a moment to question why the information has been requested when asked to provide sensitive or personal information. You should always make a judgement on what you want to divulge, and whether it is in your best interests.
- Remember that legitimate organisations such as banks and the University's IT Service Desk will never ask for your password or other access credentials.
- Keep your personal documents e.g., passport, driving licence, etc. secure always and report any losses to the police.
- Always check bank and credit card statements carefully and report anything suspicious to the bank or financial service provider immediately.
- Use a credit-checking agency (e.g., Experian) if you have any concerns.
- If possible, keep a record on how your information was provided and to whom, as this may prove useful if details subsequently become compromised but always try and use well known and reputable websites for purchasing items off the Internet.
- Always use built-in privacy and security tools (i.e., websites beginning with https:// and showing a padlock) to ensure that any shared information is appropriately safeguarded.
- Be particularly careful when opening files/attachments sent in emails as these may contain malware (malicious software) which could capture keystrokes or compromise information sent to websites.
- If using a shared/public PC's make sure that your data is not accessible at the end of your session by ensuring that it is protected by access controls or securely deleting it, especially where it may be 'cached' (saved) in a web browser.

2. Phishing

2.1 What is phishing?

Phishing is the attempt to use email, or any other form of communication, to lure users (hence the similarity to fishing) to providing sensitive/personal information which may then be used for malicious or criminally motivated purposes i.e., fraud.

2.2 How does it work?

You will receive an email requesting your assistance or requiring your urgent attention or action; it may offer a financial inducement; ask for account verification (bank accounts, University IT accounts, etc.); highlight the need to click on a generic link; claim to offer special deals/ discounts/ promotions/prizes (often in lotteries that users have never entered!), or it could merely ask you to befriend someone but all of these are an attempt to establish contact and get you to take some form of action. The next step will depend on your response; if you have already been tricked into providing your account details then the attacker may use these to obtain money, access IT systems, spread malware (malicious software) and/or compromise your device. In the rarer form of phishing, further correspondence will be exchanged to build a relationship and garner further information or access.

2.3 Why is it so successful?

Phishing attempts tend to use tried and tested social engineering techniques which tap into basic human traits like curiosity, altruism, conformity, trust, subservience, etc. and will always attempt to elicit some form of response from a user.

2.4 What steps can you take?

- Look out for some common phishing email traits (tell-tale signs):

1. it is not personally addressed to you
2. it invokes some form of urgent response
3. it contains a generic link or attachment
4. use your mouse to hover over the link to see where it will actually redirect you
5. it does not look right (poor formatting/use of English)
6. it is from a person or company that you do not know or have not had any previous contact with

- Never reply, click on any of the links contained in the email or provide any details requested.
- Never trust the 'From' field as this information can be easily spoofed or misrepresented and be very wary of using the 'unsubscribe' option (if there is one), as this will confirm the validity of the email address and is likely to result in further requests for information.
- Finally, delete the message or if you are unsure of the contents, you can always check on the authenticity of the message by contacting the IT Service Desk.

Please note that the IT Service Desk will never request password information.

The University uses filtering software to prevent most of these phishing messages being received by end-users but given their nature and the ease in which email accounts can be created a small number will invariably get through, so the main advice is to remain cautious and look for the tell-tale signs listed above.

The National Cyber Security Centre (NCSC) have created (April 2020) a special email address to report all phishing emails to, and all University IT users are strongly encouraged to undertake this: report@phishing.gov.uk

Other useful external sites:

Action Fraud - https://www.actionfraud.police.uk

Stop Scams UK - https://stopscamsuk.org.uk/159

Take Five to stop Fraud - https://takefive-stopfraud.org.uk

3. Ransomware

3.1 What is Ransomware/Scareware?

Ransomware is a type of malicious software (malware) that stops users accessing resources or data until a fee is paid.

Scareware is a type of malware that attempts to trick a user into purchasing and downloading unnecessary and potentially dangerous software.

2.2 How does it work?

Modern ransomware will make data unreadable without the user's prior knowledge or permission. This data can only be made readable by using a key, which is only provided upon payment of a fee (normally in Bitcoins). Recent examples of ransomware have been Cryptolocker, Locky, WannaCry and Cryptowall but they all work on the same principle and can encrypt data held locally on the device (C: Drive) and data held on the network/external drives.

It is University policy not to make payment for ransomware demands.

Scareware will literally “scare” the user into taking a course of action that they would not normally take. For example, a ‘pop-up’ window appears stating that malware (usually a virus or spyware) has been found on their computer, and that this can only be removed by downloading a special ‘cleaning’ program. This, special ‘cleaning’ program, contains genuine malware which is then used to infect the computer and compromise the information or user account(s).

Ransomware and scareware can take many forms (e.g., limitations on internet access, claims that users have visited child pornography sites (sexploitation) or that they are running unlicenced software) but their common denominator will be the fact that they request payment or ask the user to take some form of action.

3.3 Why are they successful?

Both methods play on people’s fears, uncertainties, and doubts by fooling them into taking actions that at first appear helpful, in the case of scareware, or target their reliance on accessing information in the case of ransomware.

3.4 What steps can you take?

Make sure that your information is backed up (so it can be recovered if compromised), and if you do receive a suspicious ‘pop-up’ window never follow the instructions until you have checked the legitimacy and authenticity of the message by contacting the IT Service Desk.

An external collaboration of cybersecurity firms and National/European agencies have created a website to offer a one-stop shop for battling ransomware - https://www.nomoreransom.org/

In addition, always ensure that your PC is running anti-virus software, which is regularly updated, and that all the applicable operating system patches are installed.

4. Safe surfing

4.1 What is meant by safe surfing?

If you follow a few basic steps when using the Internet, you can reduce the risks of becoming an on-line victim, and enjoy the benefits of safely “surfing the web” i.e. browsing websites, watching, listening and interacting with content and buying goods and services.

4.2 Why be concerned?

The Internet is vast and provides many things to many people, which can result in both good and bad experiences. In some circles, it is likened to the old American ‘Wild West’, where it is unregulated and full of potential dangers such as impersonation, financial fraud, data loss, device compromise, etc.

4.3 What should I do?

- When shopping or banking on-line always make sure that you have a secure connection (shown by a padlock symbol and a website address beginning https://) before undertaking any financial transactions.
- If possible, always use ‘trusted’ websites i.e., ones you recognise or have a physical presence (i.e., postal address, company registration, etc.) as well as an on-line one, or ones that have been recommended by a reputable third party.
- Do not respond to spam, open attachments, or click on email links from unknown and untrusted sources.

- Use a search engine (Google) is see if anybody has posted bad reviews or warnings about the website or service.
- Always check the name of the website carefully e.g., Cranfield.ed.uk is not the true address of Cranfield University (Cranfield.ac.uk).

4.4 Keep your device (PC, tablet, smartphone) protected

- Always use a fully patched legitimate operating system (Windows, Android, Apple iOS) for accessing the Internet
- Where available run an anti-virus/anti-spyware software solution which is kept up to date

The UK Government and industry provide the following websites to assist with safe use of the Internet:

Cyber Aware - https://www.cyberaware.gov.uk/
Get Safe Online - https://www.getsafeonline.org/
Stay Safe Online - https://staysafeonline.org

5. Social networking

5.1 What is Social Networking?

Web 2.0 has enabled the sharing of information across a wide platform of technologies and brought us social networking. This is primarily associated with the real-time social interactions that occur between friends and 'known' associates via Facebook, WhatsApp, Instagram, Twitter, etc. but can also be used for collaborative working, discussion forums, knowledge management and marketing opportunities with colleagues and business partners e.g., LinkedIn.

5.2 What should you consider?

As you are posting information on to a website or service that is ultimately controlled and managed by a third party you need to understand that this information could be available forever. Once posted, information may be difficult to retrieve, retract or prevent from spreading to unintended recipients, so be especially careful of replying to debates in the "heat of the moment".

Remember, the University does not control information placed on social media sites and therefore confidential or valuable IPR (Intellectual Property Rights) information should not be posted in the 'public' domain. Always assess whether the information (i.e., is it personally or commercially confidential) is likely to cause embarrassment if seen by unauthorised parties, before publishing content.

5.3 Why could social networking be harmful?

Phishing, spam, and malware distribution are known problems on social networking sites so think before you click on links, as although you may trust the source this does not mean that it has not been compromised, and if you have any suspicions don't take any action that could compromise your computer or information.

5.4 University strategy, policy, and guidelines

The University's Social Media intranet site is available here:

https://intranet.cranfield.ac.uk/CranfieldBrand/Pages/Social-media.aspx [Internal only]

5.5 How can you protect yourself?

- Think before you post and limit the personal information that you share e.g., date of birth, home address, etc.
- Check the privacy settings of the website or service to ensure that you know who you are sharing the information with, as information shared with known associates may be shared again, and again, before being passed to complete strangers. Be especially wary of invitations to 'connect' from people you do not know.
- Be careful when sharing information on your whereabouts and consider who else may be interested to know that you are on holiday, at a conference, etc.
- Turn off the GPS (Global Positioning System) function on your smartphone camera if you plan to share images online, as these will make publicise your exact location – see above.
- Keep your device up-to-date and install security patches (if available) to prevent exposure to malicious software.

UK government and industry websites on social networking:

https://www.getsafeonline.org/social-networking/social-networking-sites/

https://www.childnet.com/

Further information or advice can be obtained by contacting the IT Service Desk – **W:** servicedesk.cranfield.ac.uk; **T**: 01234 754199; **E**: servicedesk@cranfield.ac.uk or the University's Information Security Team – **E**: ITSecurity@cranfield.ac.uk

Document control

Document title	Information Security Guidance
Document number	CU-IT-ISGde-5.01
Originator name/document owner	Information Security
Professional Service Unit/Department	Information Technology
Implementation/effective date	October 2022
Approval by and date	Information Assurance Committee; 25/09/2022
Date of last review and version number	September 2023; V1.1
Date of next review	August 2024
Standards reference	Not applicable
Information categorisation	Open

Document Review

Version	Amendment	By	Date
1.1	Removal of redundant links to external sites	Information Security	4th October 2023