IT Security Guidelines

cybersecurity@londonmet.ac.uk

LONDON METROPOLITAN UNIVERSITY

Contents

Introduction 4

Information Security Awareness – Cybersecurity at Work and at Home 4

Protecting yourself 4

Strong passwords 4

Password hygiene 4

Your identity 5

Phishing 5

Protect your data 6

Backup your files 6

Anti-malware software 6

Encrypting your devices 6

Keeping software up to date 7

General awareness 7

Got infected? 7

Protect your devices 7

Separate personal and professional data 7

Securing your device physically 7

Locking your devices 8

Laptops and desktop computers 8

Mobile phones and tablets 8

Lost or stolen 8

Know your information 9

Passport 9

University website 9

Information security classification 9

Know the threats 10

Malware 10

Viruses 10

Spyware 10

Ransomware 10

Vulnerabilities 10

Phishing 10

Denial of Service 11

Know your environment 11

Rogue Wi-Fi hotspot ... 11
Shoulder surfing ... 11
Awareness ... 11
Recover from Infection ... 11
Removal of malware ... 11
Change your passwords ... 12
Future protection ... 12
Cyber Security Awareness Training ... 12
University Mandatory Training ... 12
I think I’ve fallen for a phishing scam, What do I do? ... 13
What to do if your account is compromised ... 13
Think before you click ... 14
Contact us ... 14
General awareness ... 14

LONDON
METROPOLITAN
UNIVERSITY

Introduction

Information is one of the most important assets to an organisation and all information is valuable and should be appropriately protected. Security is a combination of systems, operational procedures and internal controls to ensure integrity, confidentiality and availability of data to support the operation of the organisation.

Whether you are a student, member of staff or contractor, you all have an important part to play in protecting University systems and the information stored on them. The Cybersecurity Responsibilities and Guidelines explain those expectations, obligations, and conditions of use which you should read, understand and comply with.

Information Security Awareness – Cybersecurity at Work and at Home

Protecting yourself

Sharing with the world what you had for dinner won't hurt anyone but sharing too much information about yourself could hurt you. It's easily done, and most of the time you won't even know until it's too late. Staying safe online is becoming increasingly important, but there are lots of things you can do to help.

Strong passwords

A strong password has a length of nine characters or more, with a mixture of upper and lower case letters, numbers and special characters. Ideally, chosen completely at random. Using weak passwords that can be easily compromised is a common cause of identity theft and other cybercrimes. Cyber criminals have tools that can generate and test millions of passwords combinations per hour. The use of a strong password will reduce the risk of you becoming a victim.

Password hygiene

Do:

- consider using specialist password management software to avoid writing your passwords down, or storing them on your computer in plain text form to remember them
- if you are not using a password manager, consider using a pass phase rather than a password to make sure it's easy for you to remember, but difficult for anyone else to guess
- have a different password for each account
- change your password if you have the slightest suspicion, it has been disclosed.
- Set up and manage your password through the London Met Password Management Service

Don't:

- write down your password or store them on your computer in plain text
- share your passwords with anyone
- let applications including a web browser (apart from a password manager) remember your passwords when asked. Just click no.
- use words that are associated with yourself, such as your pet's or relative's name, phone number, or other personally identifiable information
- use commonly known acronyms or patterns such as **qwerty** or **123456**
- use the password of **password**.

A Password Policy has been provided by the University, please follow our guidelines.

It's healthy to check periodically whether your details have been disclosed because of data breach from a used vendor. A good source to check this is haveibeenpwned, where you can subscribe for any future data breach notification that include your details.

Your identity

All your personal information has value to somebody. If a cybercriminal were to obtain this, the results could be devastating.

You need to make it as difficult as possible for your identity to be stolen. Here are some steps you can take to keeping your personal information physically secure.

- When disposing of documents which contain personal data, e.g. bank and credit card statements, phone and utility bills, and other official documents, it is advisable to cross cut shred or incinerate.
- If you think your bank or credit card details have been compromised in any way, contact your bank or credit card company immediately. This includes if you've misplaced your bank card, or if expected cards have not arrived. Don't forget to sign all new cards as soon as they arrive.
- Avoid paying for anything if the transaction requires your card to be taken away from your sight for processing. In no situation is this needed and could open up opportunity for your card to be cloned. Upon paying with chip and pin always make sure no one is looking over your shoulder, known as shoulder surfing.
- Lock all sensitive identification documents such as passport, bank cards, birth certificate up in a secured container.
- Encrypt your storage media where possible, see Protect Your Data section below.
- Keep your computer hardware and storage media safe from theft or loss and if disposing of it, wipe all hard drives or other storage media using a specialist software tool.

Phishing

Phishing is the attempt to obtain sensitive information such as login credentials, banking information and personal data by disguising as a trustworthy entity via various communication methods such as emails, phone calls and websites.

The University have a training and guidance programme in place called Boxphish to help protect you and combat this threat. Please go to our Cybersecurity page for more information. It is all staff's responsibility to engage with and complete the Boxphish training programme.

Protect your data

Guidance to help you protect your data both at work and in the home environment

Protecting your data is just as important as protecting yourself, whether it is research data that costs millions of pounds to gather, the only copy of a cherished photograph or an almost finished final year project or dissertation, all information has value.

There are three pillars of information security.

- **Confidentiality** - preventing the unauthorised disclosure of information.
- **Integrity** - preventing information tampering.
- **Availability** - information can be accessed when required.

Finding the right balance for securing your data will depend on the nature of the information and its sensitivity. Most of the information security is common sense, such as:

Backup your files

Having a backup of your files allows you to recover your data should the worst happen. Backups can either use cloud-based storage (BOX for business), or an external device such as a USB hard drive that can be disconnected from a computer and stored separately. However, if you decide to do your backups, you should regularly check you can get the information back as expected.

Working on your files in BOX rather than on local copies on your laptop will ensure that they are always available and backed up.

Anti-malware software

Malware is malicious software that deliberately reduces the three pillars of information security. Anti-malware software protects you from this by continuously monitoring your computer and stopping malware from running. The University recommends using a reputable anti-malware provider and ensuring that the product is kept up to date and turned on.

All university owned and managed laptops are protected with up-to-date anti-virus software.

Encrypting your devices

Encryption is the process of converting the data on your device from readable, to unreadable until a special key is provided that only you should know. Performing some form of encryption on your device, whether it be all the disk, part of it, or file-by-file, is an extremely effective way in keeping your data secure on your device.

All university owned and managed laptops have full disk encryption.

Keeping software up to date

It is important to keep all software up to date as companies release new patches to their software to counter new threats as they emerge. This includes operating systems, applications, and anti-malware software that are updated on a regular basis. One of the most important applications to keep up to date is your internet browser, as this is your primary gateway to the internet. If your browser runs any plugins (e.g. adblockers, Java), these should be maintained in the same way.

All university owned and managed laptops have software updates applied to them automatically.

General awareness

Whilst technology can help protect your data, the number one factor is your own security awareness. Keeping yourself informed of the latest security threats is essential to help guide secure behaviour, please see below to improve your cyber awareness.

Some general advice to get started is follow your gut instinct; if something doesn't look right, seems too good to be true or doesn't feel right, stay away, think before you click! and if you're not sure, ask.

Got infected?

In the unfortunate case your computer still becomes infected with malware, head over to our "**Recover from infection**" section for more information.

Protect your devices

Guidance to help you protect your devices both at work and in the home environment

Your devices act as a gateway to your data. It is important to secure your devices, both physically and digitally as well as the data accessed online.

Separate personal and professional data

It is good practice to use separate devices to access personal and profession data. The university makes laptops available to all staff so that everyone has a secure computing environment to access their professional data, therefore it is advised not to access personal email accounts, social media or files on a university owned and managed laptop.

Similarly, it is advised not to access university data such as email, systems and files from personally managed devices, in compliance with the University Data Protection Policy

Securing your device physically

Whether it be a laptop, mobile or tablet, any portable device is vulnerable to theft, loss, or vandalism so below are a set of precautions to ensure your device doesn't get left exposed to such threats.

- Never leave your laptop or small device unattended, whether it is in the library, office and especially out in public.

- If you are going out for coffee or lunch, either take your device with you or lock your device in a location out of view. However, if there is a need for you to leave your device in an unsecured area, consider using a cable lock.

- When transporting your device, it might be worth using a low-key shoulder bag, briefcase, or backpack. Avoid expensive bags that attract attention and may highlight you have expensive contents inside.

Locking your devices

One of the best security measures you can put in place to protect your information is to use a screen lock on your devices. This can be applied to all modern-day technologies such as mobile phones, tablets, laptops, and desktop computers. All university owned and managed laptops are configured to lock after 10 minutes of inactivity.

Laptops and desktop computers

Most computers and their operating systems allow for password protected screen savers. This means that after a period of inactivity, not only does your screen saver kick in, but when the computer is awoken, your password is required before access to your data is afforded. It’s advised you have your screen saver set to initiate after a sensible period of inactivity for your needs. All university owned and managed laptops screen savers are password protected.

Mobile phones and tablets

Mobile phones and tablets can be secured in many ways. Whilst PINs are simple and easy enough to remember, usually a four number sequence isn't enough as this can be guessed. Technologies such as pattern recognition, fingerprint scanning and facial recognition are more unique to you which provides increased security.

Setting your devices to lock automatically after a short period inactivity will ensure that you are minimising the risk of unauthorised access to your device and its information. This will also reduce the amount of pocket (or bag) dialling carried out without your knowledge.

Also, modern devices either encrypt their storage by default, or provide this feature. This can protect your data and should be set up. More information can be found about encryption on the Protect your data section.

Lost or stolen

Losing or having your device stolen can be scary and potentially dangerous, which may result in unauthorised access to your data. However, there are a set of precautions you can take to protect your device(s).

- Install a 'Find my device' software/app client on your device. For Apple OS device users, iCloud provides this functionality natively.
- All University owned and managed laptops can be remotely wiped if you report yours is lost.
- Always keep your devices with you when away from the office or home.

Know your information

Information security is everyone’s business. All information has a value, irrespective of personal, sensitive, or financial data; the consequences of not looking after it could have serious implications to the University or to you personally.

Passport

Your passport is one of the most valuable documents an individual could own. In the wrong hands, it would give an attacker the ability to impersonate you. You could lose money, damage your credit rating and reputation, and in an extreme example, your house. It is the centre piece.

- **Confidentiality** - although your passport doesn't contain a huge amount of information about you, it contains enough to be able to aid an attacker in gathering information about you, which can lead to malicious attacks. This document therefore should be stored in a secure location when it is not required for use.

- **Integrity** - the integrity of your passport is the most important of the three as this covers the accuracy and trustworthiness of the data. If the integrity of your passport is damaged or defaced, it will make it void and the document will become useless.

- **Availability** - depending on how much you travel, your passport needs to be in a valid working condition and available when required, especially in cases of urgency.

University website

The London Metropolitan University’s website acts as a marketing tool for the organisation and the courses it offers.

- **Confidentiality** - the University website is available to all. The information presented is classified as public.

- **Integrity** - only certain members of staff can change the content on behalf of the organisation.

- **Availability -** the University website must be accessible as often as possible in order to be an effective marketing tool.

Information security classification

The Information Security Classification Policy sets a framework for preserving the confidentiality, integrity and availability of information assets based on their level of sensitivity and value to the University. These documents are designed to provide guidance on how to classify information assets properly as well as how to handle and store them appropriately.

Know the threats

In today's cyber world, there are many threats that only seem to be getting smarter and more advanced in their techniques. It's important to understand the dangers that are prevalent on the internet.

Malware

Malware, an umbrella term which is short for malicious software that can be annoying or harmful which may infect a computer, phone, or tablet. Attackers use malware for a variety of illegal purposes, which may include stealing usernames and passwords or preventing your devices from working properly. Malware can be installed by opening infected documents, clicking on phishing links, exploiting out of date software.

Viruses

A virus infects existing programs with the general aim of being destructive and are designed to infiltrate and gain control over a system. A type of virus, known as a 'worm' (write once, read many) can spread across computers and connected networks by making copies of itself. Another well-known type of virus is a trojan horse, which presents as legitimate software but contains malicious content.

Spyware

Spyware is a type of malware which may collect a variety of information about you and your computer system. This information could be your internet browsing history, computer usage habits, personal information or even account details. All gathered information is then often transmitted through the internet to the malicious attacker(s) without your knowing.

Ransomware

Ransomware is a type of malware that prevents or limits users from accessing their system by encrypting the files on the infected device. Generally, once the encryption process has been completed, a ransom is then presented to decrypt the files. Most anti-malware providers offer ransomware decryption tools which are available free of charge several days after the infection has been identified.

Vulnerabilities

A vulnerability is a weakness in an IT system that can be exploited by an attacker. Vulnerabilities can occur through flaws in software, internet extensions or caused by user error. Attackers will look to exploit these opportunities, often combining one or more of them to achieve their end goal. Keeping your device up to date will assist in reducing these vulnerabilities, as covered in Protect your devices section.

Phishing

Phishing is a way to gather lots of information quickly about user's credentials or provided credentials. These credentials can then be sold online and used for later attacks which may include reconnaissance into a business to find senior employees to target specifically (spear phishing).

Denial of Service

A Distributed (from more than one location) Denial of Service (DDoS) attack is an attempt to reduce the availability of an online service by overwhelming it with requests. An attacker could target a wide variety of service providers such as banks, government agencies and online entertainment retailers. The loss of revenue escalates as this type of an attack continues. If your laptop isn't secure, it could be used to launch a denial-of-service attack against someone else's network.

Know your environment

Being out in public with your device often poses more threats (both physical and digital) to your information compared to being in your home or office environment. It is also worth considering who has access to that environment, an example being young family members that wouldn't consider the value of the device and its data that they have access to.

Rogue Wi-Fi hotspot

A rogue Wi-Fi hotspot is an access point set up by a malicious user. It's meant to mimic a legitimate access point provided by a business, such as a coffee shop that provides free Wi-Fi to its patrons. Most people don't think twice before connecting to a free public Wi-Fi service.

Once connected to a rogue access point, the malicious user can eavesdrop on network traffic and potentially steal sensitive information such as account credentials and personal information. It also has the potential to provide access to your device for malicious software to be installed and run without your knowledge.

If you are unsure about a certain Wi-Fi access point, for example the wireless network requires no password or has a suspicious name. If you have a mobile phone, consider setting up a “hotspot” to connect your laptop to so it uses your mobile data connection instead, this will protect your device, as well as your data.

Shoulder surfing

If you are on public transport or in a public location, refrain from accessing sensitive information such as corporate, personal, and other confidential information as the possibility of ‘shoulder surfing’ (someone reading your screen behind you) or being overheard could occur.

Awareness

Never leave your device unattended, whether it be in the library, unsecured office and especially out in public.

Recover from Infection

If your device becomes infected with some form of malware, there are some tasks you should undertake to restore your device to a safe working state.

Removal of malware

The first stage to recovering from an infection is to remove the malware from your device. This can be achieved using specialised software which many of the industry leading anti-malware companies offer as a free solution. A few pieces of software that you could use on your device are Kaspersky Anti-Virus, Avast Anti-Virus or Malwarebytes for example.

Change your passwords

If your device has been compromised with malware, any stored credentials could have been captured by the malicious software. After removing the malware infection, you should consider changing the passwords for all your accounts. For your university account please use our Password Manager service

Future protection

- Add-ons to web browsers that can block potentially malicious adverts can be extremely useful, an example being Ad blocker.

- Two-factor authentication involves having to enter something you know such as a password and something you have, such as a one-time token delivered either to your phone or generated by a card reader. Without these two pieces of knowledge, access will not be granted.

The use of these technologies will protect you by reducing the risk of malicious pop-ups and provide an extra layer of protection in gaining access to online services.

For University support please contact the IT Support, who will:

- Help you make sure your account is fully secured
- Provide advice specific to the compromise
- Track down other users who may have been affected

For more help and information please download ‘What to do if your account has been compromised or hacked’ from our Cybersecurity Staff page or Cybersecurity Student page.

Cyber Security Awareness Training

London Metropolitan University has invested in Cybersecurity training for all staff, including temporary staff and anybody who accesses the IT systems. The training is called Boxphish. It is the member of staff’s responsibility to ensure that they engage with the training and complete the courses that they receive. Failure to engage with the Boxphish training may lead to disciplinary action.

University Mandatory Training

Mandatory training for all staff is provided through Weblearn. All mandatory training is a priority for all staff to complete. Repeated failure to complete mandatory training following reasonable management requests to do so may lead to disciplinary action.

LONDON
METROPOLITAN
UNIVERSITY

I think I've fallen for a phishing scam, What do I do?

If you, or anyone in your department, fall for a phishing scam:

1. Report to your bank immediately if any bank details are involved

2. Change your university account password - Password Manager

3. Email cybersecurity@londonmet.ac.uk who will:

- Help you make sure your account is fully secured
- Provide advice specific to the particular compromise
- Track down other users who may have been affected

4. Follow our advice to protect your account:

What to do if your account is compromised

If your account has been compromised or you have, or think you may have, clicked on a link within a phishing email and provided your University username and password, then as a matter of urgency, please visit the Password Manager Service to change your password to something significantly different.

Then email cybersecurity@londonmet.ac.uk

We also recommend that you change that password anywhere else that you have used it (such as online banking, Facebook, Amazon).

You also need to log into your university email account via a web browser and perform the following checks:

1. Go to Details (scroll to the bottom right corner) to see recent account activity. Click on Sign out of all other sessions.

2. Click on the cog icon in the top right and go to:

3. Settings - General:

- Check that your Signature and Out of Office AutoReply settings have not been tampered with - if they have, then change them back

4. Settings - Accounts

- Send mail as - Check that your account name hasn't been changed. If it has click on edit info and update this
- Grant access to your account - Are there any account names in there that you don't recognise? If so delete them

5. Settings - Filters and Blocked Addresses

- Delete any filters that you did not create yourself
- Check the details of the filter. In many cases the phishers will set a filter to delete all incoming email. If this is the case, delete the filter then check your Bin for any genuine email that has been deleted

6. Settings - Forwarding and POP/IMAP

- Remove any forwarding addresses that you have not added yourself

7. **Check Apps connected to your account** - go to Google Security Settings and remove any apps that you haven't given access to yourself.

8. **Let us know –** Visit the IT Self-Service Portal - Log a ticket or Chat with us Please also email cybersecurity@londonmet.ac.uk with the details.

Think before you click

The concept of "think before you click" is one of the most important factors in terms of information security.

When you receive an email, download a file(s) from the internet, or click on a link, think of the following:

- Is the email genuine, such as source address, spelling and context?
- Is this file(s) from a trustworthy source?
- Is the link legitimate, such as the destination of the URL?

Here are five easy rules to protect your information:

- Never disclose security details, such as your account credentials and security questions
- Don't assume an email, text or phone call is authentic. Use the internet to confirm contact details if required
- Don't be rushed. A genuine organisation won't mind waiting
- Listen to your instincts. You know if something doesn't feel right
- Stay in control. Don't panic and make a decision you'll regret.

Contact us

If you think you have given away your details to phishers, or you're unsure about a message, get in touch with us as soon as possible via the IT Self Service Portal - Log a ticket or Chat with us. Please also email cybersecurity@londonmet.ac.uk with the details.

General awareness

- Cybersecurity Staff page or Cybersecurity Student page.
- The UK Government - Cyber Aware
- The UK Government - Get Safe Online website
- Google's Stay Safe Online resources
- Microsoft's Safety & Security Centre website