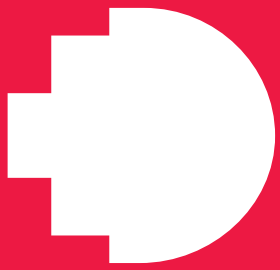
2020 Guide to staying safe online

You are the key to our cyber safety. Play your role.

What's next...

RMIT UNIVERSITY



Introduction

It's important we understand the basics of cyber security and take personal responsibility for keeping our staff, students and partners information safe. Even a single cyber incident could do huge damage to the University's reputation.

Phishing tactics and scams that play on human weakness are our greatest cyber risk. Cyber threat actors (the bad guys) continue to look for easy access to our systems, making us all targets. They succeed because not everyone is aware of the risk, or we ignore advice, which unfortunately gives the bad guys access to our systems and information.

Changing behaviours to limit our exposure to cyber risks is important. It could be an email, phone call, SMS – remain alert, be suspicious, and if your intuition says there's something wrong, listen to it!

Do not disclose any personal or RMIT information online or via email without verifying the recipient first and validating their right to have that information. Your digital world should mirror the security of your physical world. You wouldn't leave your front door open, welcome strangers into your home or leave confidential papers in your letterbox. The online world is no different.

This is the fourth edition of our annual Cyber Security Guide. Please familiarise yourself with the information, advice and tips, which are based on recent cybercriminal threats and tactics. Some simple behavioural changes may well be the difference between your own safety and wellbeing and years of regret.

Thank you for helping us to create a strong human firewall where we remain united in our purpose of staying safe online.

Tony Aramze
Chief Information Security Officer

Harry the hacker

It's another ordinary day for Harry the professional hacker. His job today is to access RMIT systems and steal sensitive or confidential information such as accounts payable and human resources.

Harry opens an email containing RMIT account usernames and passwords that he purchased from the dark web. Logging into each account, he checks which have system access. It's 'pay day' within 10 seconds – one of these accounts belongs to Sally, a senior staff member with access to HR and payment systems. As part of her role, Sally has access to authorise the creation of vendors in RMIT's vendor payment system. However, Harry is quickly annoyed to find out he needs two similarly ranking staff's approval to setup payments to his newly created vendor.

To get a second account, Harry sends out a phishing email (often used to steal user data, login credentials and credit card numbers) to other staff and students using Sally's compromised account. Masquerading as an RMIT Human Resources staff member, Harry tries to trick these staff to log-in to a fake RMIT page.

Several RMIT staff comply with his request, and after a few hours Harry has his second account. Harry now has access to create and pay his new vendors. Checking what other access he has collected, he finds he can view our HR, student records and research databases. After setting up a few vendors, Harry copies the information he thinks will be valuable. To keep his mum happy, he accesses the academic register and adds his name to the 2014 Masters graduates.

Sally, returning to work the following day, is horrified to find out that thousands of students and staff have received a phishing email from her account.

RMIT data has been compromised and our reputation may be damaged because we have lost data and jeopardised the integrity of graduation records. Your data and personal information may now be in the wrong hands.

How did this happen? While the email came from a real, but compromised, RMIT account, the URL inside of the phishing email belonged to Harry the hacker. Our colleagues failed to heed the warnings of an unexpected email asking to confirm login details and did not verify the validity of the URL address.

We all need to be cyber alert to protect our valuable information.

Learn how you can boost your cyber protection knowledge and skills through the information, advice and tips in this guide:

1 Deadlock your front door

Like your front door at home, your password secures your online world. The longer the password, the stronger it is. A passphrase or sentence, rather than a single word or an arbitrary mix of letters, numbers and symbols, makes it harder for hackers to access your data.

A passphrase uses a sequence of words in a phrase, such as Star/home-gate96:Samjack-5431. It should comprise at least four words and at least 13 characters. Aim to include upper and lowercase letters, numbers, symbols and even spaces.

But don't use the same passphrase on all your accounts – it's the first thing a cybercriminal checks on cracking a password. Passphrases also don't belong on sticky notes on your PC or in your wallet.

Think! Is your front door always unlocked?

More ways to protect your passphrase

1. **Use a password manager.**
   This is an app you can install on your computer, tablet or smartphone that helps you generate, manage and store your passwords securely. You only have to remember one passphrase, which you use to access the password manager.

2. **Use multifactor authentication (MFA).**
   This security measure requires two or more proofs of identity before access is granted to an account. It could be a code from an SMS, a token, biometrics (e.g. fingerprint), a link in an email, a random pin, or something similar. Not every business offers MFA, but all the big social media platforms do. Visit MFA set-up guidelines online.

3. **Decline prompts to 'save your password'.** This feature may leave an open door to malicious activity if your computer is compromised.

4. **Cover the keypad.**
   When entering a PIN or password in public, cover the keypad. You never know who may be able to view video surveillance of public areas.

5. **Use the 'Notify me' tool.**
   The website haveibeenpwned.com has a great tool, 'Notify me', that will send you an alert if any of your email accounts or passwords are compromised. It will also tell you where the data breach occurred so you can promptly update passphrases. Go to https://haveibeenpwned.com

Extra protection for your RMIT email account

From time to time, RMIT will enforce a password reset after a cyber incident. The reset will be much easier for you if you have set up 'self-service password reset' (SSPR). Search for 'self-service password reset' on the staff or student website.

2

Scammers lay bait. **Don't get caught!**

Phishing catches thousands of Australians

Cybercriminals are smart. They use social engineering – an assortment of malicious activities based on psychological techniques – to try to manipulate you into trusting them, so you do what they want.

'Phishing' is a technique using email, texts, social media or telephone calls that aims to trick you into revealing valuable data such as usernames, passwords, bank account and/or credit card details. The cybercrim blasts out messages to one or many email addresses or mobile numbers they have.

Emails are a primary method for phishing attacks against RMIT staff and students. Cybercriminals can 'spoof' RMIT email addresses of people you know so it looks like it comes from someone you trust and deal with regularly. Therefore, don't assume everything you receive is legitimate.

For example, cybercrims have tried to trick RMIT by pretending to be a supplier providing new bank details or sending an unexpected invoice or an email asking staff to click on a link to download an invoice – which can let them into our whole system!

Phishing works often enough for cybercrims to keep using it, so you need to be able to identify when you are being phished.

Think!

Do you welcome strangers into your home without checking who they are and what they want?

How to identify a 'phishing' expedition

There are tell-tale signs that identify a phishing message. Think S-C-A-M! when you see any of these top four tricks:

1. **Sender.** Is the sender known to you and were you expecting an email from them?
2. **Response.** Is there an undesirable impact if you don't respond?
3. **Act.** Is the request asking you to do something urgently, such as provide login or personal information, authenticate something, authorise a payment, or just click on this link?
4. **Motive.** Is the email playing to your emotions, such as panic or fear of consequences, rather than logic?

The dangers lurking in email

However, no matter how good the phishing email looks, it can't hide everything. If you have any doubt about the legitimacy of an email, here are some more detailed checks you can do to see if you are being phished.

1. **Check the email's domain address.** The domain address is the part that comes after the '@' symbol, e.g. rmit.edu.au. Is it legitimate? Use your web browser to see if the domain name actually exists. DO NOT use any link in the email to check the domain address.

   When checking a domain address, the correct domain needs to appear after the https:// and before the first '/'. In most cases, anything after the first single '/' can be disregarded and is often used by scammers to confuse you (see phishing image example).

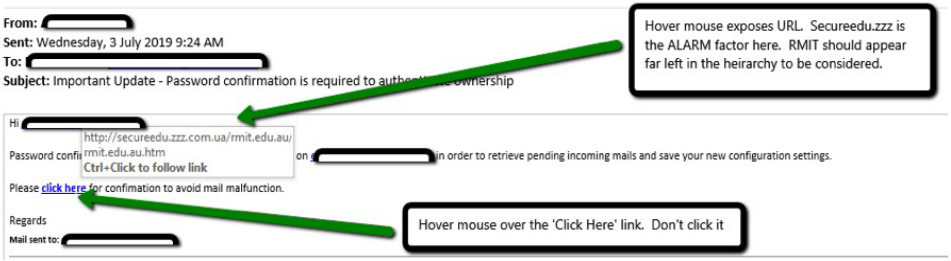
2. **If it is an RMIT address, validate it.** Use an RMIT directory search to find the contact details of the 'sender'. Call them via telephone or Skype to verify if they sent the email and made the request. DO NOT use 'Reply' on the email to contact them.
3. **Check the 'From' field.** Any email where the 'reply to' address is different to the sender's address ('From' field) is phishing. If in doubt, check at https://isitphishing.org

Send us your phish!

Forward all suspicious emails received in your RMIT mailbox to **reportphishing@rmit.edu.au** If it is found to be malicious, our cyber experts will take the necessary action to contain the risk.

Here's what phishing emails look like

This is an image of real phishing email. By hovering your mouse cursor over the 'Click here' link the real URL is displayed. **DO NOT CLICK.**



This email is from secureedu.zzz.com.au and NOT rmit.edu.au. The 'rmit.edu.au' domain name should be immediately after the 'http://' and before the first '/' in the address. It is shown here as the second domain listing, which is part of the deception. The discrepancy means it is a phishing email and should NOT be opened.

RMIT uses filter tools to help weed out bad emails, attachments and known phishing emails and to verify links as safe before they get to your inbox. However, no tool is perfect. If an email looks suspicious to you, then there's a good chance it is. Don't click on any links, do more in-depth checks, and if you have any doubt forward it to **reportphishing@rmit.edu.au**

Sharpen your detecting skills

- Practise your phishing awareness skills at https://phishingquiz.withgoogle.com
- Keep an eye out for our dedicated detection honing skill sessions, which will be held throughout the year across campuses.

For more details, go to **rmit.edu.au/**cybersecurity

Quick phishing checklist

1. Were you expecting the communication (email, text message, phone call)?
2. Is the sender asking you to provide information? (Requesting you to check or confirm login details on your account; requesting a payment; wanting an update to bank account details?)
3. Is there a sense of urgency?
4. Is the sender asking for information that is inconsistent with their role or need to know?
5. Is the sender asking you to open an attachment or access a website via links in the email sent?
6. Is the link legitimate? (Hover your cursor over the link and check the address.)

TIP

- Never enter your username and password into a website where you have been directed by a link in a message, particularly email and SMS messages.
- Don't disclose your login details through an email, SMS or over the phone TO ANYONE. No legitimate organisation will ask you to do this.

3

A pledge to **Personal protection**

There are several ways, in addition to your password, you can improve security when using internet connections, applications and devices.

Internet connections

1. **WPA2.**
   Set your home router to WPA2, rather than WPA, so you have the highest security and encryption standards available. Refer to your router's user manual for instructions.

2. **Public WiFi.**
   Public WiFi is generally not secure, even if you have to use a security code to access it. Don't use it to access any personal information or accounts as this may allow other people to gain access to it. Treat the WiFi at cafes, airports, hotels, shopping centres or similar as unsafe; only use it for activities such as general browsing of sports, weather and news. Only use secure or trusted connections – such as RMIT WiFi, your home network or Eduroam* – to access sensitive accounts such as online banking.

3. **Entering sensitive data online.**
   If you need to provide sensitive information online, check the URL starts with 'https' or has a padlock symbol in the address bar. This signifies you have a secure connection.

4. **Security tips**.
   More tips to ensure your home WiFi and internet connections remain secure can be found on the Australian Government's Stay Smart Online website at:
   https://www.staysmartonline.gov.au/
   Search: Wi-Fi and internet connections

Think!

Your front door may be locked but are your windows and other external doors open?

Applications

1. **Review your application settings.**
   Turn off anything not required, especially settings that give unnecessary access to your calendar, camera, contacts, location, microphone, storage and telephone.

2. **Turn on multifactor authentication.**
   (also called two-step verification). Use MFA on Office 365, Google and any personal accounts or applications you access. MFA double-checks you are the person you are claiming to be and provides a greater level of security. You'll find the option to switch on MFA in the security or privacy settings of your online accounts.

3. **Use App Store and Google Play.**
   Download apps and upgrades from Apple's App Store or Google Play only. Do not install apps, certificates or any executable file from links in emails, social media, text messages or pop-up ads.

4. **Review your privacy settings.**
   After every software or application upgrade, review your privacy settings. An upgrade may put your settings back to default and give unauthorised access to your contacts, photos, camera or other features.

Devices

1. **Automatic updates.**
   Set your smartphone, tablet, laptop and desktop for automatic updates of the operating system.

2. **Disable auto-connect.**
   WiFi and Bluetooth auto-connect should be disabled when not in use.

3. **Safeguard your devices.**
   Keep your devices with you at all times. Do not leave devices unattended in public, in a hotel room or in a car. Even leaving devices in a hotel safe is not recommended.

4. **Cables and adapters.**
   Only use cables and adapters purchased from reputable retailers to charge your devices. Malware can be easily transferred to your device by using another person's accessories or those purchased from non-reputable dealers.

5. **Avoid public USB ports.**
   Free USB ports for device recharging are often available in airports and hotels. However, they can easily transfer malware to your device and compromise your data. Stick to your device's power adapter and cable and use a standard electrical power point.

6. **RMIT computers.**
   If you are using an RMIT computer that is constantly on, restart your machine once a week to allow new software to be installed and help keep your data safe.

*Eduroam is a secure WiFi network available in many Australian and international educational locations.

4

Spilling the beans

Protect and respect sensitive data.

Store and share data safely

RMIT provides staff and students with excellent tools that enable safe storage, sharing and access to electronic files through OneDrive, SharePoint and myDesktop.

OneDrive file storage

OneDrive app

OneDrive files can be accessed on your mobile devices. Download the OneDrive app from the App Store (iOS) or Google Play (Android).

All staff and students are provided with an Office 365 licence, which includes cloud storage in OneDrive and SharePoint. This means you can store work and study-related files for easy access from any device, without multiple copies floating around.

The University recommends that personal work-related files such as drafts and works in progress be stored in OneDrive.

RMIT staff can share OneDrive files and folders to enable colleagues to access files. Staff can also use a new feature in Office 365 to classify information using data protection sensitivity labelling. This allows you to transmit, store and give others access to data based on its sensitivity.

To access OneDrive, use your RMIT email address and network password to log in via https://portal.office.com, then select ‘OneDrive’.

Think!

Do you leave your personal information lying in the street?

SharePoint sites

SharePoint app

SharePoint folders can be accessed on your mobile device. Download the SharePoint app from the App Store (iOS) or Google Play (Android).

SharePoint is a useful site for files that require shared access for a team or workgroup. Separate sites are recommended for each unit or workgroup. Every SharePoint site comes with a 'documents library', where you can set up folders and manage who can access your team's files.

Setting up a 'public site' means ALL RMIT staff and students will have access to the content, so be careful when uploading documents. Don't upload documents containing sensitive information to a site with 'public' settings. Make sure the folder's settings only allow access to the people you choose.

myDesktop

myDesktop is a secure virtual RMIT desktop that automatically gives you access to your files as if you were on campus. It can be accessed from any browser, anywhere. Go to mydesktop.rmit.edu.au and log in with your email address and network password.

myDesktop is ideal for working or accessing RMIT files on a public PC but be sure to disconnect (log off) once you've finished so others can't access your information.

THE DANGERS OF PORTABLE STORAGE DEVICES

USBs and flash drives are not a safe storage option for sensitive information as they are easily lost. Others may unknowingly share a USB stick that carries a malware infection, which can then infect a computer when inserted into a port.

Planting infected drives in carparks, airports, events or streets is a tactic used by cybercriminals. Resist the temptation of a freebie if you see one lying around.

5

Harm's way is a **dangerous journey**

Stay protected when travelling

Travelling overseas makes you more vulnerable to cybercrime; about 20 per cent of travellers experience some form of cybercrime. Similar to when you leave your home, taking a few extra precautions will help reduce your risk.

Before you leave

Download software updates. As well as being cheaper, it also means you have the best protection available.

During your journey

Plan to use your smartphone as a secure internet connection for your laptop. Learn how to do it, buy a suitable international roaming data plan, and avoid large downloads so you don't incur excess data charges. This precaution will mean you won't need to use unsecure public WiFi.

Take all your electronic devices, including any security tokens, onboard with you when flying. Always store your security token separately from your device, such as in your coat pocket or personal carry-on luggage, rather than the laptop case.

Think!

Do you travel overseas and leave your oven or iron on?

However, if you are travelling to a destination where there may be data interception by the country's government, we recommend that you do not travel with any devices. If you are travelling for RMIT work purposes, loan laptops and mobile devices can be booked through the Service Desk. As long as roaming is available in the destination country, the device will come with a suitable international roaming data plan.

On the ground

Bluetooth connectivity in rental cars may leave your device vulnerable to hackers. Personal information such as contact lists may be retained even after a connection has been terminated so it's best not to connect your phone to a rental car.

When you get home

Defer your social media travel posts until you are safely home and be sure to restrict the visibility of your posts to people you trust.

MORE TRAVEL TIPS

For more travel tips, see the international travel pages at **rmit.edu.au**/cybersecurity

6 I'm sensitive and I'd like to **stay that way**

Respect data privacy and confidentiality

Around your workstation

Many staff deal with sensitive or confidential information at their workstations. It's our responsibility to protect this information and the privacy and confidentiality of the people about whom this information is about.

When you are finished with a confidential paper document, return it to its secure location (e.g. lockable cabinet), shred it, or put it in the confidential waste bin for secure disposal. Don't leave it visible on your desk while you are at a meeting or getting lunch, and certainly not overnight.

Your workstation should be locked when you are away from it. You can lock it by holding the Windows and 'L' key together. You are responsible for any activity done under your username, so lock it before you leave it.

Think!

Do you keep your blinds open at night?

Email and social media

1. **Classify and protect according to sensitivity.** Office 365 allows RMIT staff users to classify emails and documents according to the sensitivity of data. To find out more on how to use this feature, go to **rmit.edu.au**/staff/services-and-tools/its/passwords-and-security/data-protection

2. **Update group email lists.** If you manage a group email list, update its records immediately when a colleague leaves or changes role. Using outdated lists may put confidential data into the wrong hands and result in regulatory fines against RMIT.

3. **Be careful using email auto-prompts.** Auto-prompts are an easy way to populate an email address field, but it's also easy to select an incorrect name from your sender list. Sensitive data can be easily compromised.

4. **Take care with social media posts.** Images with computer screens, notice boards or people in the background have unwittingly compromised security and confidentiality when posted on social media.

Think!

Start your journey here.

7

#Security pilgrimage

Cyber safety checklist

You've now got the latest information to help thwart the cybercriminals who are constantly looking for a way into RMIT's computer systems. Here's a summary of the security measures discussed in the previous pages.

Don't take the bait

Think **S-C-A-M**:

- **Sender** – Is the sender known and is the email expected from them?
- **Consequence** – Is there an impact if you don't respond?
- **Act** – Is the request asking you to do something?
- **Motive** – Is the email playing to your emotions, such as panic or fear of consequences, rather than logic?

Deadlock the door

- **Switch to passphrases.** Make your RMIT password a strong passphrase of at least 13 characters.
- **Make it unique** to your RMIT login.
- **Never share it** with anyone.
- **Set up** Self Service Password Reset for your RMIT login.
- **Use a password manager** to securely manage your passwords.

Take the pledge

- **Avoid public WiFi**
  except for browsing news, sports and weather.
- **Enter sensitive information**
  only if the URL starts with 'https' or has a padlock symbol in the address bar.
- **Turn on MFA**
  (multifactor authentication) in your Office 365 and wherever it is offered in an online account.
- **Review application and privacy settings**
  whenever an app is updated.
- **Use App Store and Google Play directly.**
  Do not install anything from links in email, social media, texts or pop-up ads.
- **Set automatic updates**
  for your mobile devices' operating systems.
- **Disable auto-connect**
  for WiFi and Bluetooth when not in use.
- **Avoid public USB ports to recharge.**
  Use your own power adapter, cable and a standard electrical power point.

Stay out of harm's way

- **Download software updates**
  before you go.
- **Use your smartphone**
  as a secure internet connection for your laptop.
- **If data interception**
  is likely to be a problem (staff), book RMIT loan devices.
- **Don't use Bluetooth**
  to connect to rental cars.
- **Social media posts**
  should be left until you get home.

Safeguard the beans

- **Use OneDrive**
  to store work and study files for easy access from any device.
- **Use SharePoint** (staff)
  to share files for a team or workgroup. Remember that a 'public' SharePoint site can be seen by ALL RMIT staff and students.
- **Use myDesktop**,
  RMIT's secure virtual desktop, to access your RMIT files from any browser, anywhere. Remember to log-off when you're finished.
- **Be wary of USBs.**
  They can easily transmit malware once plugged in and 'lost' USBs are a favourite ploy of cybercriminals.

Close the blinds

- **Confidential documents**
  should be secured in lockable cabinets or securely disposed of after use. Do not leave them on your desk when at a meeting or out at lunch.
- **Lock your workstation**
  when you are away from it. You are responsible for any activity under your username.
- **Classify and protect**
  sensitive data and emails using a new Office 365 feature.
- **Update group email lists**
  when a colleague leaves or changes role.
- **Email auto-prompts**
  make it easier to select the wrong name from a sender list.
- **Backgrounds matter**
  in social media posts.

8

Help,
I need somebody!

RMIT Service and Support is HERE

All staff and students are encouraged to report any suspicious online requests or incidents that may lead to a data breach as soon as possible.

Forward any suspicious emails (phishing) to: reportphishing@rmit.edu.au

For help or to report a data or security incident, contact: RMIT ITS Service and Support Centre

rmit.edu.au/its/ithelp

+61 3 9925 8888

- To book a **cyber awareness team briefing**, email RMIT Information Security Office
- To become a **Cyber Ambassador** or to learn more about our Ambassador program, email RMIT Information Security
- **Join us on Yammer:** RMIT Cybersecurity Awareness
- For more information on cyber security including useful links and tips refer: **rmit.edu.au**/cybersecurity

Think!

Call the experts. If you mess up, 'fess up.
We won't judge.

Help external to RMIT

Australian residents

Financial fraud: Contact your bank or financial institution. If you've sent money or your personal banking details to a scammer, contact your bank or financial institution immediately.

For more financial security tips and information go to: commbank.com.au/security

Identity theft:
Contact IDCARE, a free government-funded service.

Scam victim: SCAMWATCH and ACORN (Australian Cybercrime Online Reporting Network)

Sign up for free scam alerts and keep updated on the latest threats to Australians to help minimise your risk of becoming a cyber-victim at the Australian Government's Stay Smart Online website: https://www.staysmartonline.gov.au/alert-service

Vietnam residents

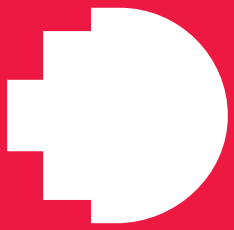
Contact the Vietnam Computer Emergency Response Team, http://www.vncert.gov.vn

Consult the Police Department for High-Tech Crime Prevention (under the Ministry of Public Security).

Contact the Authority of Information Security.

Barcelona/European residents

Go to Europol at https://www.europol.europa.eu/report-a-crime/report-cybercrime-online and select the link for your country.



Remember, data never sleeps and
the internet doesn't forget.