UCT FAQs

Q1. What happened?

On 17 August 2022, UCT's Information Communication & Technical Services (ICTS) identified that a limited amount of personal information had been exposed to malware on an isolated Directory machine.

Q2. When did this happen?

On 17 August 2022. UCT contacted affected individuals as soon as we practically could after this date once we had completed our preliminary investigations.

Q3. Do you know who tried to access the information?

Incidents like this are generally carried out anonymously; it is often not possible to identify with certainty who may be behind incidents like this.

Q4. What exactly was accessed?

The data held within the Directory includes the personal information of staff members, students, alumni, and third-party contractors. The nature of the information relates to the data subject's names, surnames, email addresses, telephone numbers, staff numbers, staff job titles, student numbers, and password hashes.

Q5. What measures can I take to protect myself, do I need to switch accounts or passwords?

- As a precautionary best-practice, measure we strongly recommend that you change your UCT account password and do so regularly. We suggest that where you may have used the same password for personal accounts, that those passwords also be changed. Prior to this incident UCT has been in the process of finalising a password policy that will require UCT account holders to have a 16-character password, and users are encouraged to follow this principle.

- Do not click on any links or open any emails from unknown or suspicious sources.

- It is good practice to always be vigilant of any unusual requests in relation to your personal information or the various accounts you may hold.

- Should you suspect that your identity has been compromised or that you have been a victim of fraud, apply immediately for a free Protective Registration listing with Southern African Fraud Prevention Service (SAFPS). The SAFPS is a non-profit organisation focused on fraud prevention and financial crime. The SAFPS assists in preventing fraud and impersonation as a result of identity theft to protect the public from associated financial consequences. Its Protective Registration service alerts SAFPS members, which includes banks and credit providers that your identity has been compromised and that additional care needs to be taken to confirm that they are transacting with the legitimate identity holder.

Q6. What can be done with the information that has been accessed?

Although it is generally low-risk information that has been impacted, we encourage you to take the necessary steps to protect yourself, as set out in our notification and explained above.

Q7. What steps will UCT take to protect my information in the future?

As a result of this incident UCT has taken the following steps:

1. the machine on which the malware was located has been isolated and taken offline
2. a full review of Active Directory security controls is being undertaken
3. work is underway to restore, or possibly rebuild our Active Directory; and
4. We are in the process of resetting service and administrative accounts with additional security policy measures in place.

We will remain alert to any further issues which may arise as a result of this investigation.

Q8. How did this happen?

Our system was the subject of unauthorised access. We have taken steps to address this with a view of preventing similar incidents taking place in future.

Q9. Why was I not told sooner?

We sought to inform all affected data subjects as quickly as we practically could. We had to carry out investigations into the incident to understand its extent before getting in touch with you.

Q10. Do I need to take additional personal security precautions?

Yes, there are some steps that we recommend, as set out in our notification, and explained above.

Q11. I've heard you've lost data, was I affected too?

If you have not received a notification from UCT advising that you were affected by the incident, then you have not been affected by this.

Q12. How do I notify the South African Police Services (SAPS) about this incident?

If you would like to inform the SAPS about the incident and how it might affect you, contact should be made with your local police station. Generally speaking, SAPS will only expect to be notified of the issue if you have evidence of criminal activity.

Q13. Have you notified SAPS?

We have notified the Information Regulator, in terms of the Protection of Personal Information Act. At present, there is no indication that the incident requires notification to the SAPS.

Q14. Who can I speak to?

If you have any questions or concerns about this matter, please do not hesitate to contact UCT's IT Helpdesk.