



Cyber Incident Reporting

Cyber incidents are events that threaten the confidentiality, integrity, or availability of digital information or information systems. Unreported cyber incidents can result in significant damage to the affected party.

Accordingly, victims are encouraged to report to Rwanda-Computer Security Incidents Team (Rw-CSIRT) all cyber incidents that may:

- result in a significant loss of data, system unavailability (denial of service), or an authorized control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on critical information technology systems;
- affect critical infrastructure or core government functions;
- have impact national security, economic security, or public health and safety or
- result in organizational financial loss and reputational damage.

All users are encouraged to immediately report to the Rwanda-Computer Security Incident Response Team (Rw-CSIRT), any suspicious online activity or cyber incident for fast and appropriate action and advice. By reporting such computer security incidents to Rw-CSIRT, the system administrators and users will receive technical assistance on how to resolve such incidents.

This also helps the Rw-CSIRT to correlate accurately the incidents reported and analyze them; draw inferences; disseminate up-to-date information; and develop effective security guidelines to prevent the occurrence of such or similar incidents in the future.

What can I report to Rw-CSIRT?

Cyber incidents that may be reported include:

- phishing (users receiving suspicious emails);
- hacking (such as unauthorized access to one's own device)
- denial of service
- malware and viruses
- ransomware (encrypted files or devices)
- website defacement
- spamming
- unauthorized access to computer systems
- compromised email accounts
- sextortion
- user identity theft
- attacks on computer systems and any other cyber security related incidents



How to report an incident to Rw-CSIRT

Cyber security incidents can be reported via Rw-CSIRT website www.cyber.gov.rw/report-incident/ through the online reporting form as well as at Rw-CSIRT's office.

Incidents should not be reported from a machine which you think is infected.

For proof of identity, the incident reporting party should bring their Identity Card.

In case the individual with a report cannot report the incident personally, then he/she can authorize another person to report on their behalf, with an authorization letter duly signed, and ID card or power of attorney. The incident reporting party should preserve all the available information without any alteration.

Enquiries about incidents can be made through Rw-CSIRT Hotline: **9009** or by email at incident@ncsa.gov.rw.

What follows after reporting the incident?

After reporting the incident, the incident reporting party will immediately (as soon as the incident is received) receive an acknowledgment email.

The reporting party will be informed when the incident is resolved or if any other information or clarification is required.

What should not be reported to Rw-CSIRT?

The following IT issues should **NOT** be reported to Rw-CSIRT:

- Forgotten passwords or blocked/locked accounts by systems or system admins
- VOIP services not working correctly (e.g. Zoom)
- Hardware problems
- Network connection problems (e.g. limited/exhausted bandwidth, slowness, etc.)
- Printer issues
- Any other non-cyber security-related issue(s)

For actions that require legal intervention and investigation, the reporting party should contact Rwanda Investigation Bureau (RIB), [Cybercrime unit](#).