Cyber Security Incident Reporting

A cyber incident is an event that could threaten the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to Government institutions and the private sector. 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 un 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; or
- have impact national security, economic security, or public health and safety.

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 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 future.

What can I report to Rw-CSIRT?

Incidents that are reported include phishing, hacking, denial of service, malicious code (malware, viruses, ransomware), website defacement, spamming, unauthorized access, compromised email accounts, sextortion, identity theft, and attacks on computer systems and any other cyber security related incidents.

How to reach and report an incident to Rw-CSIRT?

Cyber security incidents can be reported via Rw-CSIRT website (https://cyber.gov.rw/rw-csirt/ through the online reporting form as well as at Rw-CSIRT's office.
For proof of identity, the incident reporting party should bring their Identity Card.
The victim only must report an incident or in case the person may not be able to come personally, then he/she can authorize any other, together with an authorization letter duly signed and ID card or power of attorney.
Enquiries about incidents can be made through Rw-CSIRT Hotline: **9009** or by email at **incident@ncsa.gov.rw.**
A child or minor must be accompanied by their parents.
When reporting an incident online, users should also provide the following information if relevant to the nature of the incident:

Examples:
Fake or hacked accounts – the name of the account and URL
Compromised Email accounts – User ID
Ransomware – infected machine
Phishing – Phishing link, phishing email, email headers
Denial of Service or Distributed Denial of service attack – IP address
Unauthorized access – logs

Malware – malicious file, link or email
Website defacement – website link
Unauthorized video – link of the video
Spam – email header
Service unavailability ---name of the system
The incident reporting party should preserve all the available information without any alteration.
Incidents should not be reported from a machine which you think is infected.

What follows after reporting the incident?

After reporting the incident, the incident reporting party will 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 legal actions, the reporting party should contact Rwanda Investigation Bureau (RIB), Cybercrime unit.