Recovery after Malware Incidents

Objectives:

At the end of this episode, I will be able to:

Understand what the main goal of recovery after Malware Incidents should be for the IH&R team.

Explain what the recovery steps IH&R personnel should follow after a malware incident are.

External Resources:

Recovery after Malware Incidents

Recovery steps should be based on the four main elements of prevention, awareness, vulnerability mitigation, and threat mitigation.

What are the recovery steps that an incident responder has to follow after a malware security incident? -

```
▪ Wipe the hard disks and other impacted portable storage media such as memory
cards and USB drives

▪ Reimage and rebuild the compromised systems from scratch to avoid presence
of malicious code

▪ Restore the backups of the system only after ensuring that the backup data
has no traces of malware by testing it with updated antivirus software

▪ Scan all the devices and systems with antivirus that contains the malware
signatures

▪ Restore email services after blocking the malicious senders and change the
passwords of compromised accounts before using

▪ Enable scanning of links and attachments in all the emails passing through
the server

▪ Disable automatic file sharing between the systems

▪ Restore data from synchronized cloud services after scanning

▪ Uninstall and install a fresh copy of an affected application

▪ Restore the system functions including disabled/enabled services and
open/closed ports to their original state
```