Once you think that the infection has been removed, change the passwords for your online accounts and check your banking activity. Report anything unusual to your bank and, as needed, to your local law enforcement authorities.

Learn how to protect your computer from future infections and avoid data loss.

- Run a full scan of your device and remove the threats by using security software.
- Install security software from a trustworthy source.
- Disconnect your device from the network as soon as possible, in order to prevent additional malicious activity.
- Ensure that your internet connection is unusually slow.
- Ensure that your security software and operating system are up to date.
- Be wary while browsing the internet and do not click on suspicious links, pop ups or dialogue boxes.
- Unknown processes are running in your system (visible in the Task Manager, Processes tab).
- Only download apps and software from sources you can trust.
- Keep your web browser up to date and configured to alert you whenever a new window is opened or anything is downloaded.
- Cover your webcam when not in use.
- Do not click on links or attachments within unexpected or suspicious emails.
- Unknown programs are installed on your device (visible in the Control Panel, Add or Remove Programs).
- Regularly back-up your data.
- Your files are modified or deleted without your permission.
- INFECTED? WHAT TO DO NEXT

Once you think that the infection has been removed, change the passwords for your online accounts and check your banking activity. Report anything unusual to your bank and, as needed, to your local law enforcement authorities.

Learn how to protect your computer from future infections and avoid data loss.

- Your internet connection is unusually slow.
- Unknown processes are running in your system (visible in the Task Manager, Processes tab).
- Unknown programs are installed on your device (visible in the Control Panel, Add or Remove Programs).
- Your files are modified or deleted without your permission.
- PROTECT YOURSELF

- Regularly back-up your data.
- Be wary while browsing the internet and do not click on suspicious links, pop ups or dialogue boxes.
- Keep your web browser up to date and configured to alert you whenever a new window is opened or anything is downloaded.
- Do not click on links or attachments within unexpected or suspicious emails.

- INFECTED? WHAT TO DO NEXT

Once you think that the infection has been removed, change the passwords for your online accounts and check your banking activity. Report anything unusual to your bank and, as needed, to your local law enforcement authorities.

Learn how to protect your computer from future infections and avoid data loss.

- Your internet connection is unusually slow.
- Unknown processes are running in your system (visible in the Task Manager, Processes tab).
- Unknown programs are installed on your device (visible in the Control Panel, Add or Remove Programs).
- Your files are modified or deleted without your permission.
- PROTECT YOURSELF

- Regularly back-up your data.
- Be wary while browsing the internet and do not click on suspicious links, pop ups or dialogue boxes.
- Keep your web browser up to date and configured to alert you whenever a new window is opened or anything is downloaded.
- Do not click on links or attachments within unexpected or suspicious emails.

INFECTED? WHAT TO DO NEXT

- Disconnect your device from the network as soon as possible, in order to prevent additional malicious activity.
- Install security software from a trustworthy source.
- Run a full scan of your device and remove the threats by using security software.