DON'T OPEN THAT ATTACHMENT

HOW THE FOLLINA VULNERABILITY WORKS

HOW DOES FOLLINA WORK?

YOU RECIEVE AN EMAIL FROM AN UNKNOWN SOURCE AND OPEN THE ATTACHED .DOC OR .RTF

Malicious hackers send out millions of emails with fake attachments that exploit the CVE-2022-30190 vulnerability also known as Follina.

DON'T OPEN THAT ATTACHMENT

ONCE THE MALICIOUS EMAIL IS OPENED IT RUNS A SCRIPT IN THE BACKGROUND

The fake document attachment exploits a vulnerability in Microsoft Office allowing it to run a script that gives hackers access to your device.

WHAT WILL IT TAKE?

EVERYTHING IS AT RISK.

Hackers can take over control of your computer gathering information in the background, tracking your keystrokes for passwords, or gain access to your company network.

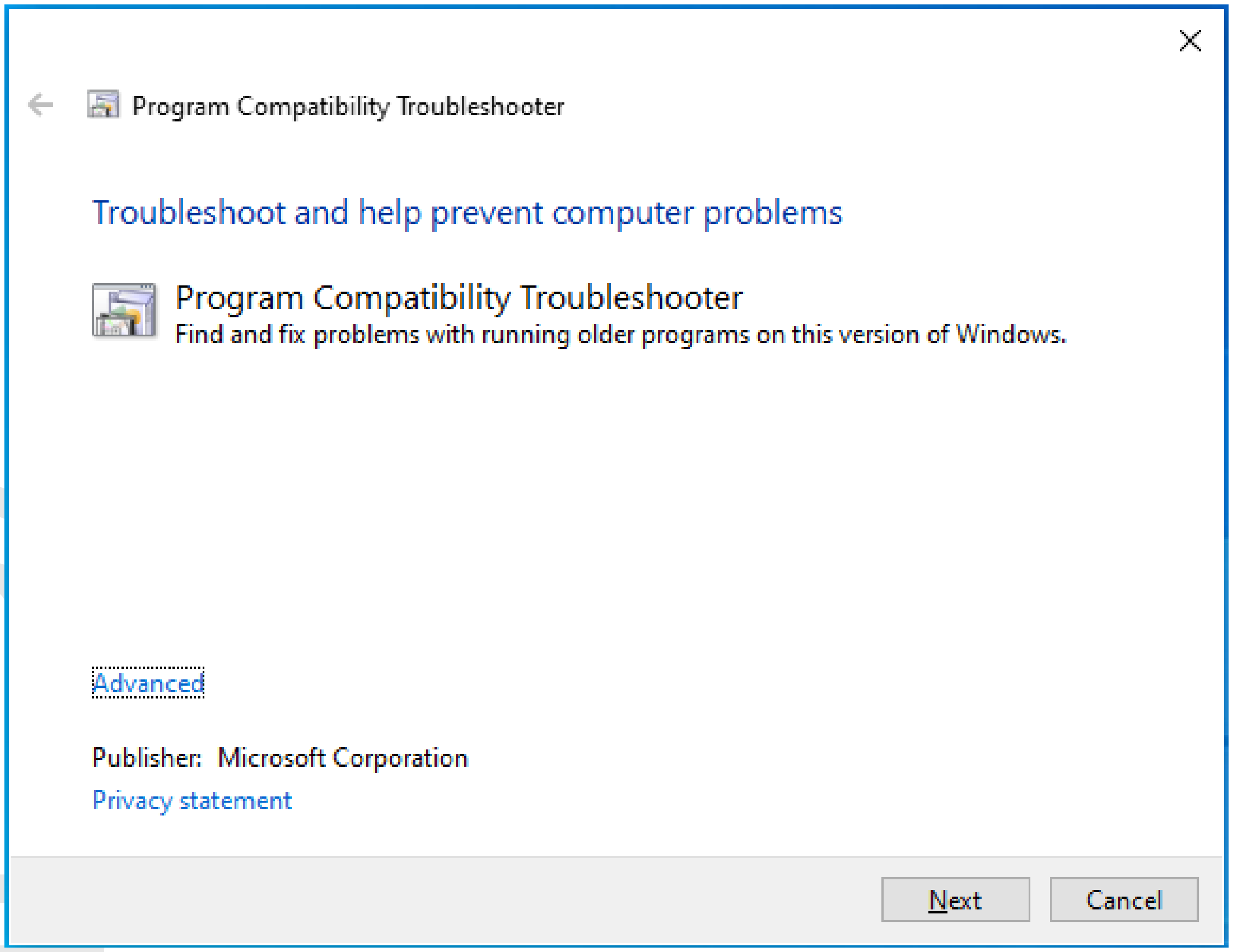
HOW DO I PROTECT MY DEVICE?

DON'T OPEN EMAILS FROM UNKNOWN SENDERS

Since there isn't a patch to fix this vulnerability yet, users must be vigilant when opening emails. Only open email attachments from trusted sources.

HOW DO I KNOW MY DEVICE IS COMPROMISED?

THIS SHOWS UP WHEN YOU OPEN A MALICIOUS .DOC OR .RTF ATTACHMENT



Program Compatibility Troubleshooter

Troubleshoot and help prevent computer problems

Program Compatibility Troubleshooter

Find and fix problems with running older programs on this version of Windows.

Advanced

Publisher: Microsoft Corporation

Privacy statement

DKBINNOVATIVE IS PROTECTING THEIR CLIENTS

PROACTIVELY WORKING TO SOLVE PROBLEMS

DKB has best practices in place that will reduce the chances of malicious emails getting through and we put mitigations in place to stop Follina even if you did open a dangerous attachment.

IS YOUR COMPANY SAFE FROM FOLLINA?

CALL US TODAY

DKB
innovative