BLOG POST

Updating our malware & ransomware guidance

Here's what's changed in the NCSC's guidance on mitigating malware and ransomware.

Emma W

We recently updated our mitigating malware guidance; it's now called **Mitigating malware and ransomware attacks**. We also took the opportunity to retire our standalone ransomware guidance. This blog post explains what we changed, and why we did it.

Two becomes one...

Having two separate pieces of guidance was confusing for some of our customers. Most of the **ransomware** content was the same in both pieces of guidance, but the **malware** guidance was slightly more up-to-date. So we have tried to make things easier by providing a single piece of guidance, with all the most up-to-date advice in one place.

New content on offline backups

We improved the guidance by emphasising *offline* backups as a defence against ransomware. We've seen a number of ransomware incidents lately where the victims had backed up their essential data (which is great), but all the backups were online at the time of the incident (not so great). It meant the backups were also encrypted and ransomed together with the rest of the victim's data. We've previously published a blog post recommending offline backups, but recent incidents suggest we need to emphasise the importance of this in our guidance as well.

Tidying up and sweeping down

While we were updating the guidance, we took the opportunity to remove some of the more detailed technical content, as feedback showed that customers tend to find these parts less useful. The new guidance is not only shorter, but hopefully more relevant.

Finding information in a hurry

Some people have already pointed out that since ransomware is a type of malware, saying 'malware AND ransomware attacks' isn't 100% accurate.

However, not everyone who visits our website knows that. Furthermore, they might well search for the term 'ransomware' (rather than 'malware') when they're in the grip of a live ransomware incident. We want to be as helpful as possible to the people who need our guidance in a hurry. The best cyber security advice in the world is useless if nobody can find it.

For the same reason, we used 'attacks' rather than 'infections', 'incidents' or 'compromises' - as we know this is by far the most popular search term. These technical trade-offs are sometimes necessary, because the NCSC needs to make sure the language used in its guidance matches what's being used in the real world.

Do you like the new guidance? Let us know! Tweet us @NCSC or email the enquiries team.

Emma W
Head of Guidance, NCSC communications

WRITTEN BY

Emma W

PUBLISHED

26 February 2020

WRITTEN FOR

Public sector

Cyber security professionals

Large organisations

PART OF BLOG

NCSC publications