National Cyber Security Centre
a part of GCHQ (/)

Threats in scope (Cyber Essentials scheme)

Created: 06 Feb 2017
Updated: 06 Feb 2017
An outline of the types of threat and the level of defence that are assessed under the Cyber Essentials scheme.

Threats to mitigate

The Cyber Essentials scheme addresses the most common Internet-based threats to cyber security — particularly attacks that use widely available tools and demand little skill. The scheme considers these threats to be:

- phishing — and other ways of tricking users into installing or executing a malicious application
- hacking — exploiting known vulnerabilities in Internet-connected devices, using widely available tools and techniques
- password guessing — manual or automated attempts to log on from the Internet, by guessing passwords

The Cyber Essentials scheme is **not** designed to mitigate against:

- attacks that require physical access to a device
- attacks that require interception of particular communications links, whether wireless or not
- attacks that exploit non-public vulnerabilities
- denial of service (DoS) attacks (for more information see Mitigating Denial of Service (DoS) Attacks(/guidance/mitigating-denial-service-dos-attacks))
- insider attacks in which an authorised user abuses their access (for more information see Mitigating insider risks with IT security(/guidance/mitigating-insider-risks-it-security))
- attacks using stolen credentials to defeat authentication mechanisms

Types of controls

The Cyber Essentials scheme covers only the **essential steps** to mitigate the above threats. Also, the scheme:

- only recognises preventative technical controls
- does not include detective or recovery controls

The scheme requirements do **not** consider whether a management regime is in place to maintain these protections.

Topics

Cyber strategy(/topics/cyber-strategy)

Was this information helpful?

We need your feedback to improve this content.

Yes No