Guidelines for Registrars on handling reported .ie domain technical abuse

The guidelines below have been drafted to assist Registrars in handling reports of technical abuse relating to .ie domains under their management which they receive via the Netcraft reporting service, or otherwise.

The guidelines are not designed to be prescriptive. Registrars may have existing protocols in place, and may take any alternative/additional steps, and provide any advice that they deem appropriate in order to support the registrant in addressing and resolving the reported abusive issue.

If you suspect that a domain is being used in a way which breaches the rules of the .ie namespace, or presents a risk / danger to the .ie DNS or its users, you may use the domain status functionality within the Registry's TITAN systems to temporarily remove the .ie domain in question from the zone whilst you investigate the matter. These domain status features are subject to certain fair use rules, which are detailed here.

Abuse Category	Description	Recommended Action Steps
Malware	Malware refers to software that is used/distributed with malicious intent. It is used by cyber attackers to gain access or cause damage to a computer or network, and/or to gather sensitive/personal information.	We advise that you check if the domain has been compromised. If you suspect that it has, you should contact the registrant to alert them to the issue. **If you are hosting the domain**, we recommend that you work with the registrant to clean up any infected files/accounts, change all passwords and make sure that all software on the server is up to date. **If you are not the hosting provider**, we recommend that you help the registrant identify their hosting provider (where possible), and recommend they take the above steps with that party.
Phishing	Phishing is a method of collecting personal information using deceptive e-mails and websites. Phishing messages usually appear to come from well-known organisations. The messages will typically ask a user to click on a link which brings them to a fake site that appears to be legitimate where important	We advise that you check if the domain has been compromised. If you suspect that it has, you should contact the registrant to alert them to the issue. If you suspect that the domain is being used in connection with illegality, we recommend that you alert the registry. Otherwise, we recommend that you alert the registrant (as deemed appropriate), and take the steps outlined below:

	sensitive/personal information will be requested— such as a credit card number, an account number or a password.	**If you are hosting the domain,** we recommend that you work with the registrant to correct this matter, remove any incorrect information from the domain and follow best practice for any bulk email marketing on the domain. **If you are not the hosting provider,** we recommend that you help the registrant identify their hosting provider (where possible), or recommend that they take the steps outlined above with that party.
Compromised	A compromised domain is one that has been made vulnerable due to unauthorised/third party access. This means that the domain is under the control of a third party.	We advise that you check if the domain has been compromised. If you suspect that it has, you should contact the registrant to alert them to the issue. **If you are hosting the domain**, we recommend that you work with the registrant to correct this matter, clean up any infected files/accounts, change all passwords and make sure that all software on the server is up to date. **If you are not the hosting provider**, we recommend that you help the registrant identify their hosting provider (where possible), recommend that they take the steps outlined above with that party.
Technical Abuse	Technical Abuse is general term that is used to identify an issue. Examples of technical abuse are cryptojacking, ransomware, viruses, hacks and other ever-evolving threats. The issue may be one of the other categories.	We advise that you investigate why the domain use has been reportedly identified as abusive (in a manner that is likely to be considered in breach the rules of the .ie namespace). If you suspect that it has, you may wish to consider **suspending** the domain using the domain status functionality within TITAN, or alerting the Registry about the party potentially endangering the .ie DNS and/or its users. **If you are hosting the domain**, we recommend that you work with the registrant to address/stop to abusive matter, and provide any related support or advice. **If you are not the hosting provider**, we recommend that you help the registrant identify their hosting provider (where possible), or provide any related advice and support.
Command and control	This is when a domain is acting as a control centre for a botnet. A botnet is a number of compromised computers running one or more bots. Botnets can be used to perform Distributed Denial-of-Service (DDoS) attacks and send spam.	We advise that you investigate why the domain has been reportedly identified as being registered for the purpose of command and control. We advise that you check if the domain has been registered for this purpose. If you suspect that it has, you may wish to consider suspending the domain using the domain status functionality, *or alerting the Registry and An Garda Síochána about the party potentially endangering the .ie DNS and/or its users.*

Spam	This domain has been used in connection with the sending of spam or is linked to spam activities. Spam refers to the mass sending of unsolicited emails and may occur in conjunction with phishing or the offering of illegal goods/services.	We advise that you check if the domain has been compromised. If you suspect that it has, and that it is being used in connection with technical abuse, such as phishing, we recommend that you follow the steps above, for instances of phishing. If you suspect that the domain is being used in connection with illegality, we recommend that you alert the Registry. Otherwise, we recommend that you alert the registrant (as deemed appropriate), and take the steps as follows:- **If you are hosting the domain**, we recommend that you work with the registrant to correct the matter, following best practice for any bulk email marketing on the domain. **If you are not hosting the domain**, we recommend that you help the registrant identify their hosting provider (where possible), recommending that they take the steps outlined above, with that party.