NOTICE & TAKEDOWN SERVICE
NTDS

NOTICE & TAKEDOWN SERVICE

Cybersprint's Notice & Takedown Service (NTDS) takes care of active threats to your organisation or brands. After having identified potential threats, Cybersprint's platform will take the Notice & Takedown request out of your hands, to help you eliminate the threats as soon as possible. Examples of threats that can be eliminated using the NTD Service:

/ Fake websites

/ Phishing websites

/ Fake social media accounts
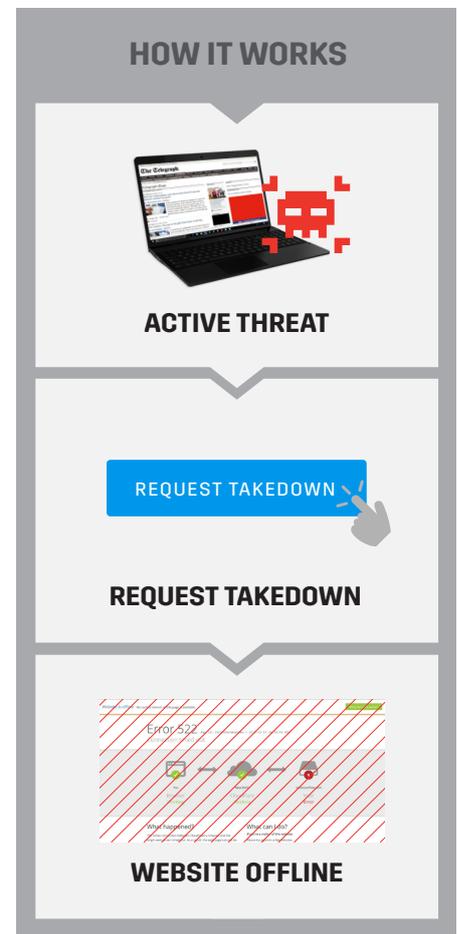
/ Fake win campaigns

/ Fake mobile apps

68%

of people consume information via a third-party platform instead of at a direct source.[1] That is why fake websites are so dangerous.

WHY IS IT IMPORTANT?

Takedown procedures through legal departments will cost your organisation too much time and money. Meanwhile, the reputation of your business is suffering while fake websites impersonate you, putting your clients, employees and vendors at risk of being scammed.

Notice & Takedown (NTD) procedures consist of contacting relevant parties and convincing them to cease supporting activities related to a threat. Examples of parties involved are:

/ Website hosting provider

/ Email hosting provider

/ DNS hosting provider

/ Domain registrar

/ Social Media platform operator

HOW IT WORKS

ACTIVE THREAT

REQUEST TAKEDOWN

REQUEST TAKEDOWN

WEBSITE OFFLINE

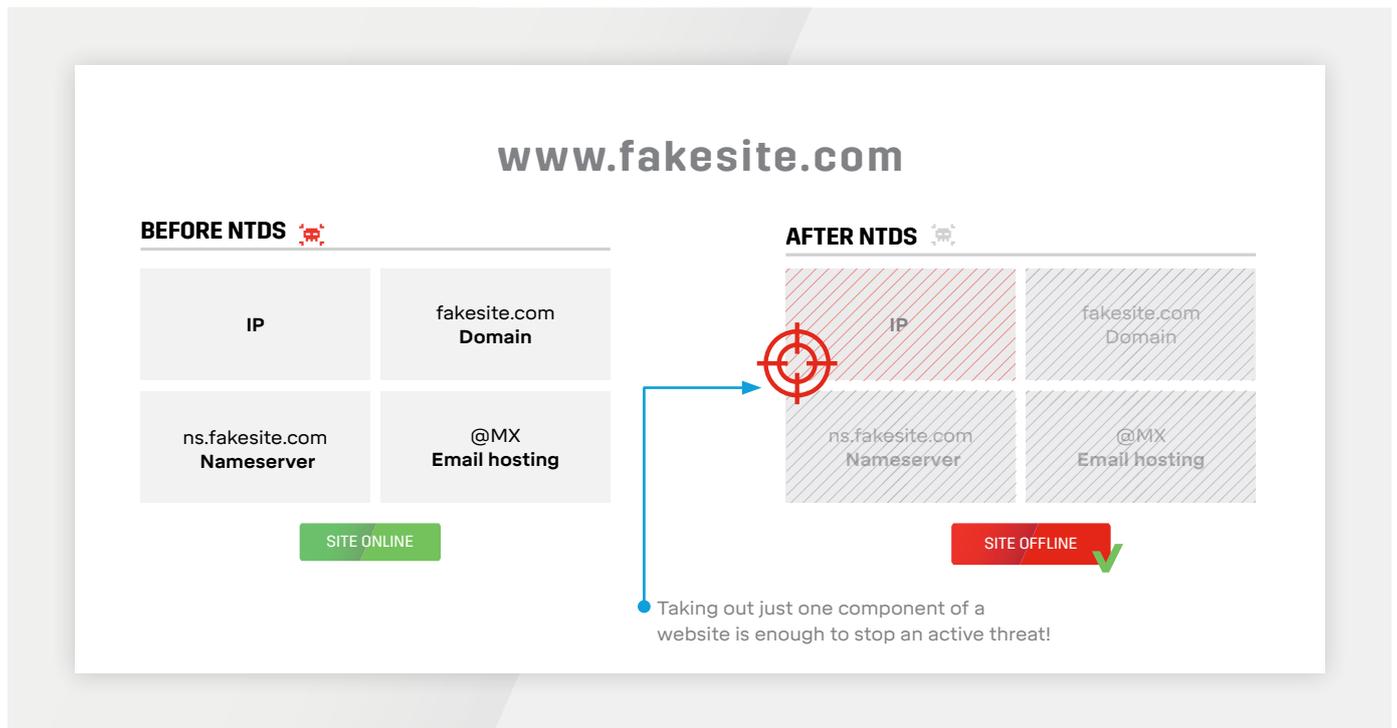"Cybersprint's Notice & Takedown Service provides a swift method to take out online threats"

NOTICE & TAKEDOWN PROCEDURE

The core component of Cybersprint's Notice & Takedown Service (NTDS) uses the internet's universal takedown procedures. NTD measures can take effect when a service provider is asked to stop providing certain services to a third party, for example with:

/ Abuse of brand components on a website or social media account

/ Active spreading of malware

/ Obvious phishing activity

/ Providing incorrect information (wrong WHOIS information)

1/3

of consumers would close their account after a digital breach.[2]

www.fakesite.com

BEFORE NTDS

IP	fakesite.com **Domain**
ns.fakesite.com **Nameserver**	@MX **Email hosting**

SITE ONLINE

AFTER NTDS

IP	fakesite.com Domain
ns.fakesite.com Nameserver	@MX Email hosting

SITE OFFLINE ✓

Taking out just one component of a website is enough to stop an active threat!

HOW CAN CYBERSPRINT HELP?

Cybersprint's Digital Risk Protection platform offers solutions to help you find and eliminate online threats. We provide real-time, actionable insights into the malicious campaigns and the ways in which cyber criminals try to abuse your brand. Cybersprint will take care of the takedown request for you, so you retain your trusted reputation.

This prevents cyber criminals from reaching your clients, employees and vendors with phishing emails, and from imitating your organisation when they target third parties.

Are you under attack? Contact us today to take down the threats you are facing. We can help you protect your organisation by successfully taking down malicious websites, fake social media accounts and other threats.

1 https://ec.europa.eu/jrc/communities/sites/jrccties/files/
dewp_201802_digital_transformation_of_news_media_and_the_
rise_of_fake_news_final_180418.pdf

2 https://www2.deloitte.com/content/dam/Deloitte/uk/
Documents/consumer-business/deloitte-uk-consumer-review-
nov-2015.pdf