CoreSentinel

PHISHING

Takedown Process

CONGRATULATIONS, you just won a trip to the Bahamas!

Update your password now!

Please confirm your account information.

You have a tax refund waiting for you.

These are the common introductory statements you can find on phishing emails or phishing sites. In this day and age where all transactions involving credit cards could be done online, phishing is becoming more common. It's necessary for IT practitioners to **know how to take a phishing site down** to protect their company's information and to prevent scammers from using their details for fraudulent activities.

The following process works very effectively in having phishing sites taken offline, suspended, and blocked by browsers and content filters - usually within 24 hours.

STEP 1

Examine the fraudulent email for malicious domain links and email addresses and take note of them.

STEP 2

Forward the original phishing email to the following email addresses:

- phishing-report@us-cert.gov
- reportphishing@apwg.org
- reportphishing@antiphishing.org
- phish@phishtank.com

STEP 3

Copy the malicious URL of the phishing site and use it to report to the following anti phishing services:

- Google: https://www.google.com/safebrowsing/report_phish/?hl=en
- Symantec: https://submit.symantec.com/antifraud/phish.cgi
- Eset: http://phishing.eset.com/report
- PhishTank: https://www.phishtank.com/
- Microsoft: https://support.microsoft.com/en-us/kb/930167
- Netcraft: http://toolbar.netcraft.com/report_url

STEP 4

Use the web based GeekTools Whois http://geektools.com/whois.php to look up the phishing domain and take note of the details. (You can also use the whois command from within linux.) The output will look something like this:

```
whois penetrationtestingtools.com.au
Domain Name:                    penetrationtestingtools.com.au
Status:                         ok
Registrar Name:                 Domain Directors

Registrant:                     TARRANT, MARK J
Eligibility Type:               Sole Trader
Eligibility Name:               TARRANT, MARK J
Eligibility ID:                 ABN 50456849980

Registrant Contact ID:          IN1439883084858
Registrant Contact Name:        Mark Tarrant
Registrant Contact Email:       Visit whois.ausregistry.com.au for
Web based WhoIs

Tech Contact ID:                IN1439883085064
Tech Contact Name:              Mark Tarrant
Tech Contact Email:             Visit whois.ausregistry.com.au for
Web based WhoIs

Name Server:                    ns1.onlydomains.com
Name Server:                    ns2.onlydomains.com
Name Server:                    ns3.onlydomains.com
DNSSEC:                         unsigned
```

Top of Form
Bottom of Form

Specifically we are looking for details of;

1. Name Servers
2. Registrant & Registrar
3. Abuse contacts

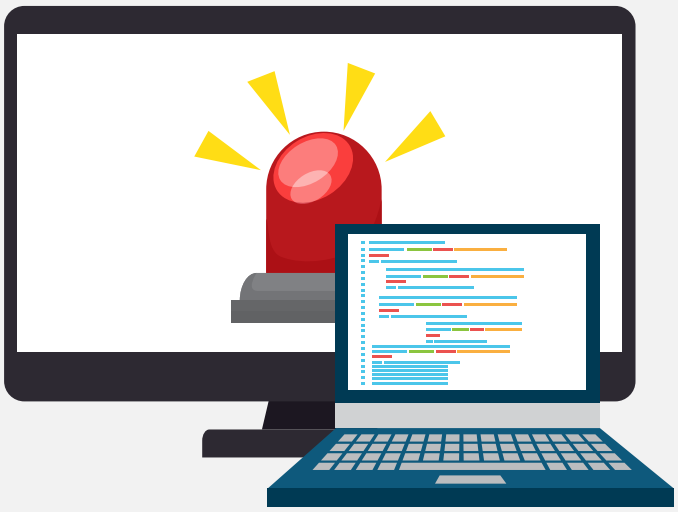
The name servers are normally associated with the organisation where the website is hosted, and this is the most important contact for a successful suspension of the account so we will **repeat the whois lookup process on the name servers** to find out how to contact them.

STEP 5

For malicious domains, contact the hosting service and the domain registry to notify them of the scam, requesting that they take action to suspend the account or take it offline. Often this email is sent to abuse@<company_domain>. Follow up with a phone call to both the hosting service and the domain registry with the request

STEP 6

Often with phishing sites, the actual domain is a legitimate business whose website has been hacked due to system vulnerabilities. The attacker uses this vulnerability to upload their phishing site to a subdirectory of the legitimate website. (And this illustrates why performing a penetration test on a website is a good idea so that the vulnerabilities can be found and patched before they are exploited by criminals.)



In this case where a legitimate business site has been hacked;

- **Contact the business;**
- **Notify them of the phishing site hosted on their domain; and**
- **Ask them to take action to remove it**

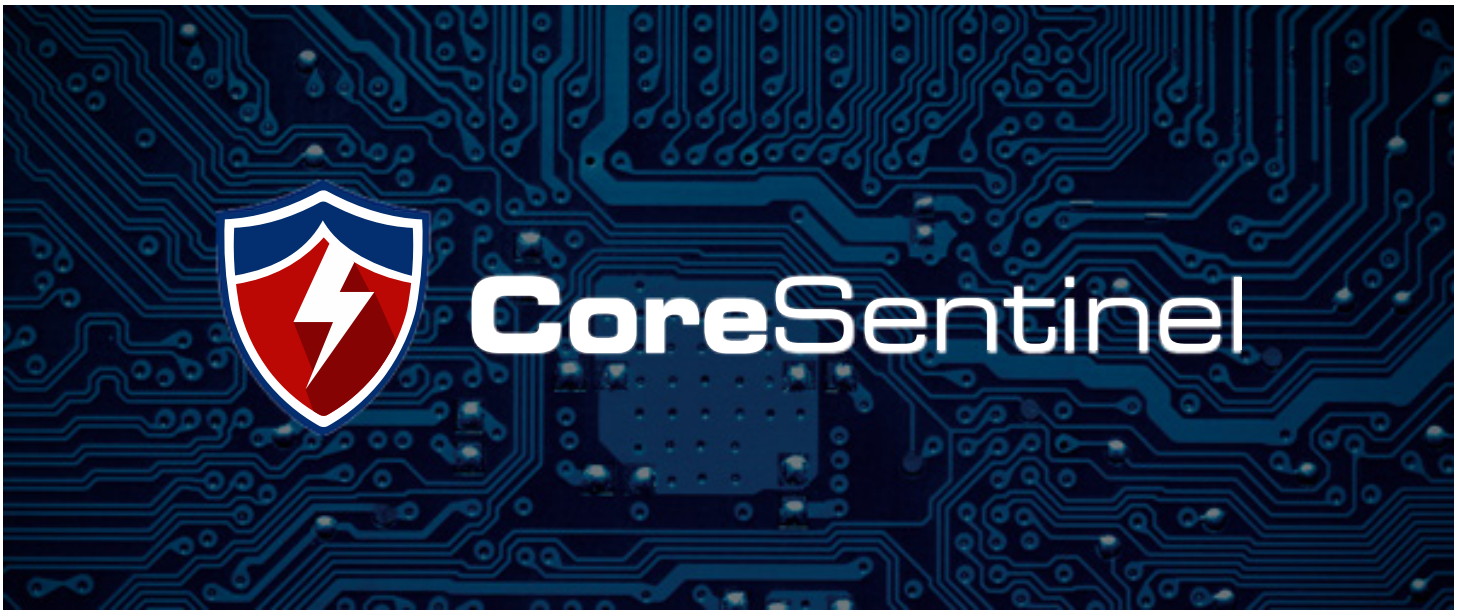
Where possible, it is also worth asking the business owner to provide a zipped up copy of the phishing site code for further analysis. Analysing this code can lead to further investigation as to how the phished data is processed, and provide more information for investigation such as email addresses in the code.

STEP 7

For malicious email addresses identified, contact the email provider and notify them of the email address/account which is being used for fraudulent purposes. This is often as simple as sending an email to abuse@<email_provider_domain>.

Our final advice to you is be wary of suspicious sounding messages. And if you suspect that a website is not what it purports to be, LEAVE immediately. Perform the procedure outlined above, and have the website taken down if found to be malicious.

Also, if you've been hacked or if the security of your website has been compromised, **seek expert assistance.**



Core Sentinel's mission is to help businesses, institutions, and organisations **stay a step ahead of hackers**. Our penetration testers are OSCE, OSCP certified and, CREST-qualified. Our consultants have worked for some of the world's biggest brands, in a range of industries, including banking, finance, insurance, health, utilities, oil & gas, government and defence.

We are the ones with the right knowledge, tools and experience to guide you to the recovery of your website.

Call us today!