Website Protection Guidelines

1. Overview

The purpose of this guide is to help Website administrators to secure their website and develop a response plan to deal with a website hacking or malware incident.

Incident Management - Preparation

- Build a Team - Create an Incident Response Team to deal with security incidents. These members should include host provider, system administrator etc.

- Register your site with Googles webmaster controls. Google will monitor sites for vulnerabilities, badaware and if discovered will contact the registered owner.

- Know your systems and controls - Document and catalogue your systems. E.g. Host details, IP address(s), Admin and other account details, Data stored, Log files (e.g. operating system event logs, application specific logs and intrusion detection system logs.), back-up and restore procedures. Please see Appendix for details.

- Use tools to review the health and content of your website. This will enable better security of the systems and also better preparation and knowledge if a system is compromised. Please see Appendix for details.

- Communication plan – Ensure you have the details of stakeholders (e.g. host providers, IT Services, Incident Response Team contact details, Data Protection Office, legal etc.). Decide on the method of communication to the stakeholders and communicate the appropriate response to them about the incident.
  Please see Appendix for details.

Incident Response Procedure

Contact the members of your Incident Response Team

- Inform your web host that your site has been compromised
- Gain a general idea of the type and severity of attack. You should gather at least enough information to begin communicating it for further research and to begin containing the damage and minimizing the risk.
- Record your actions thoroughly. These records will later be used for documenting the incident.

Quarantine your site

- Take your site offline so that it no longer serves content to users
    - This may be completed by your host provider or you, depending on system setup.
- Perform thorough user account management
    - You will require the ability to view all users, delete users, and change all passwords related to your account as required.
    - Blocking (and logging) of unauthorized access
- Closing particular ports and mail servers

For more details, please go to

https://developers.google.com/webmasters/hacked/docs/quarantine_site

Contain the incident

To stop the incident spreading to other areas you need to contain it which can be done by using Googles Search Console which includes the following:

- Verify ownership of your site using Google Search Console
- Check that the hacker didn't already verify ownership in Search Console and make unwanted settings changes.

- Determine the nature of the attack. The information in the Message Center and Security Issues in Search Console can help determine whether your site was compromised to Spam, Phish or to distribute malware.

For more details, please go to
https://developers.google.com/webmasters/hacked/docs/use_search_console

Identify the vulnerability

- Determine the attack point of origin.
- Identify the systems that have been compromised and how. E.g. Virus-infected administrator's computer, Weak or reused passwords, Out-of-date software, Permissive coding practices, SQL injections
- Identify the files that have been accessed and determine the sensitivity of those files

For more details, please go to

https://developers.google.com/webmasters/hacked/docs/vulnerability

Clean and maintain your site

- Installation of the latest, most secure version of software
- Removal of user-visable URLs created by the hacker
- Removal of unnecessary or unused applications or plugins that could make your site more vulnerable in the future
- Restoring content of site with "clean" content and eliminating the hacker's content
- Fixing the root cause vulnerability exploited by the hacker
- Changing all passwords
- Removing temporary constraints imposed during the containment period
- Installing patches and tightening network perimeter security, such as firewall rulesets
- Planning to keep your site secure

For more details, please go to

https://developers.google.com/webmasters/hacked/docs/clean_site

Review your systems and get back online

- Testing systems thoroughly – including security controls
- Confirming the integrity of the systems and controls
- Finally request a review from Google to have your page or site unflagged as dangerous or possibly deceptive to users.

For more details, please go to

https://developers.google.com/webmasters/hacked/docs/request_review

Additional resources for compromised websites

https://www.stopbadware.org/hacked-sites-resources

Appendix

Incident Response Team Contact Details

Website Details	*URL address(s)*	*IP Address(s)*		
Description of Site				
Incident Response Team				
Role	Name	Work Phone No.	Mobile Phone No.	Email
Site owner				
Host Provider				
Systems Administrator(s)				
Legal & Compliance				
Communications				
Date	*Please fill in the date the form was completed or last updated. The form should be updated at least once a year*			

Know Your Systems and Controls

Administrators of a website service should ensure that they know the IT Infrastructure of their systems. This includes the proper configuration/ patch managements, appropriate access and security controls are in place and document and catalogue their systems. This will enable better security of the systems and also better preparation and knowledge if a

system is compromised. Details such as the following should be included:

- Host provider details
- Systems architecture – platform used, web applications, other applications, services used etc.
- IP address(s) details
- Ensure all login pages are using HTTPS only
- Manage Accounts Authentication
    - Admin and other account details
    - Principle of Least privilege
    - Enforce the creation of strong passwords
- Ensure proper configuration/ patch managements
- Establish logging standards and procedures
    - Configure systems to record the right events
    - Monitor these events effectively
    - Maintain sufficient historical data (as logs can be overwritten or have insufficient storage space)
    - Make appropriate event logs available to investigators in a suitable format.
    - Review log activity and audit the logs for exceptions
- Data stored on system and the data classifications of that data (UCD Data Classification can be found here http://www.ucd.ie/itservices/ourservices/documentsandstorage/userfileguide/)
- Minimize the level of data processed
- Never upload content using an insecure channel (like FTP). Use an encrypted channel like SFTP
- Verify your back-up and restore procedures
- Document program source codes and ensure that documentation is maintained and kept up-to-date.
- Implement secure remote access
- All machines administering the website must be secure using up to date antivirus, operating systems and application are fully patches and firewall is enabled. See our device recommendations on www.ucd.ie/itsecurity "Protecting your device".
- Establish secure defaults

Tools and Websites

- http://www.ucd.ie/itsecurity
- Google website diagnostic
- https://www.stopbadware.org/files/best-practices-responding-to-badware-reports.pdf
- https://www.stopbadware.org/my-site-has-badware

- Redleg's file viewer can help you check for malicious redirects, malicious scripts, and other badware
- Unmask Parasites scanner
- Sucuri Site Check
- SparkTrust scanner
- Web Sicherheit scanner (German/English)
- Desenmascara.me (Spanish/English)
- Virus Total URL scanner and file scanner
- HEAnet Plesk User Guide -http://www.heanet.ie/wordpress/wpcontent/uploads/2014/10/HEAnet-Plesk-Panel-User-Guide.v1.7.pdf
- Wordpress Hardening - http://codex.wordpress.org/Hardening_WordPress
- https://zeltser.com/cheat-sheets/

Communication Plan

Notification to stakeholder should include:

- Type and magnitude of the incident
- Steps taken to identify the source and impact of the incident
- Whether the incident has been successfully mitigated
- What steps remain to be taken to mitigate risk
- Estimated timeline to complete mitigation in order to eliminate additional risk or exposure to the state.