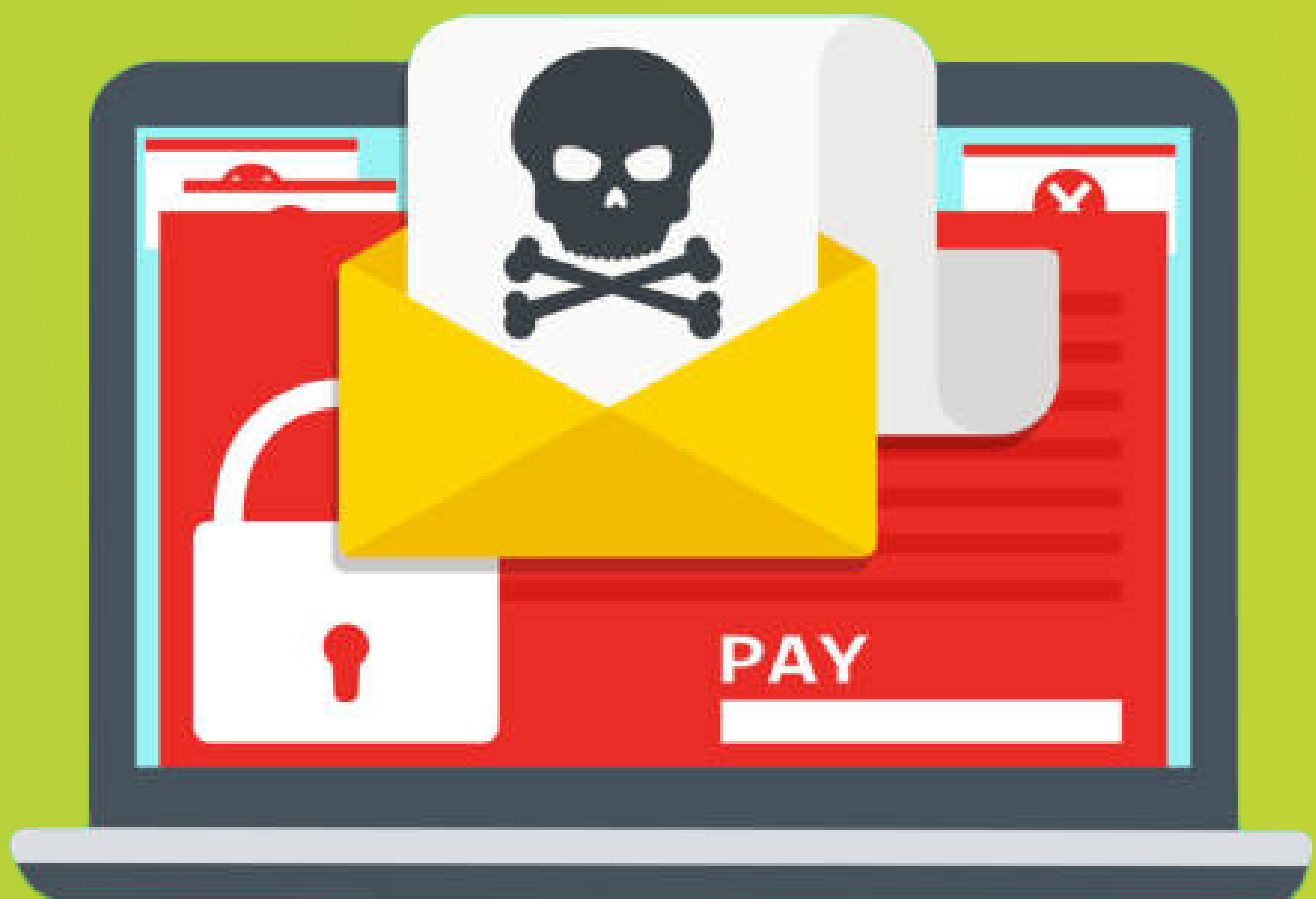


TIPS TO STOP MALWARE FROM INFECTING YOUR WEBSITE





According to statistics, [28% of data breaches](#) involve the use of malware.

Malware is defined as a type of computer software designed to disrupt or damage a system, data, or personal information.

Malware can create significant problems for your website as they often are used by hackers trying to steal sensitive data from you, such as intellectual property.

In this article, find out how you can identify and prevent malware from infecting your website.

How Does Malware Work?

Malware is designed to disrupt the operation of a computer system or cause damage. Hackers often use malware to steal sensitive data such as intellectual property from you. Malware can be transmitted to other computers in several different ways:

1. Opening an infected email attachment
2. Visiting an infected website
3. Having a computer or mobile device compromised by malware, such as ransomware

How Is Malware Spread?

Malware is spread in several ways, making it difficult to protect your website from being infected. Some of the ways used by an attacker to spread malware include:

1. Opening an infected email attachment
2. Visiting an infected website, such as one that has been compromised through malware injection
3. Having a computer or mobile device infected by malware, such as ransomware
4. Clicking on fake internet ads

How to Prevent Malware from Attacking Your Website

Perform Regular Site-wide Scans

Scanning your site for malware and malicious code regularly ensures that you can get rid of malware before it has the opportunity to cause any damage.

Scanning for malware can be done by using an antivirus, antimalware, or a website security scanner. You should perform the scan regularly, such as once a week.

Restrict File Uploads on Your Website

Your website runs the risk of acquiring malware through the uploading of images or files.



Hackers may upload malicious scripts to your site through areas on your website that allow for file uploads.

Allow file uploads only to specific areas on your website. Upload files that have been scanned for malware before doing the upload.

Keep All Software, Plugins, and Applications Updated

Often, malware infects a website because the software installed on your site is outdated.

Keeping all applications up to date ensures that there are no exploits or bugs in the software that may cause your site to be compromised.

Make sure that you host your website with a reputable hosting company that uses up-to-date software and reputable servers.

Use Form Validation

You can avoid the injection of malware through your website's forms by performing form validation. Validation ensures that information entered into a form is accurate and doesn't contain any malicious code.

Proper encoding rules are enforced when a form is validated to ensure that no special characters are inserted.

Use SSL to Encrypt Data

SSL encrypts data transmitted between your website and the end-user, which helps prevent hackers from eavesdropping on your data.

When the user types in sensitive information, such as credit card numbers or passwords, it is encrypted before being sent to the server.

Use SSL on your website to better protect sensitive data from being intercepted by hackers or malware.

Install a Web application Firewall

A web application firewall is a firewall that protects your website from malware.

Typically, a web application firewall is configured to allow some traffic but block other types of traffic, such as malicious traffic.

Install a web application firewall to help prevent your website from being attacked by malware or other types of malicious code.

Web application firewalls protect your website from attacks that cripple your website by overwhelming your hosting resources.



It monitors all the traffic between a client and server, inspecting data packets for signs of malware or malicious traffic.

Use Strong Login Credentials

Your website username and password are the first line of defence that should help you prevent malware from infecting your website.

You should always use strong passwords that other people cannot easily guess.

Additionally, you may want to consider using two-factor authentication for your account.

Use Website Security Tools to Keep Your Website Safe

There are many tools available to help you protect your website from malware.

You can use these tools to keep your website safe and protect it against malware attacks.

Web security tools actively look for malware in the code of your website and on your directory.

Some of the most common web security tools are

1. Sucuri
2. Scan My Server
3. OpenSSL

Regularly Backup Your Website

A data backup of your site's files can help you restore any lost or damaged data in case of a breach.

Regularly back up all of the website content to ensure that everything will be backed up.

If you use a WordPress site, for example, backup plugins are available to help with the process of backing up your site.

Install Antivirus Software

Antivirus software provides solutions to malware infection on your website. By using antivirus on your computer, you can scan, identify, and remove malware on your computer. Antivirus software is a must-have to help protect your website.

References

<https://blog.netwrix.com/2020/06/12/malware-prevention/>

<https://cyberthreatportal.com/how-to-prevent-malware-attacks-on-website/>