Is Your Website Phishing for Somebody Else?

How to Detect and Prevent Phishing Kits

What is a Phishing Kit?

A phishing or phish kit is a pre-created set of files a hacker with limited technical knowledge can upload to a targeted website. Phish kits make hijacking your website much easier for hackers, and thus much more prevalent. The coders who make the kits also make quite a lot of money from them. Phishing kits can mimic the login pages of other sites, stealing your credentials and then sometimes redirecting you to the real site so you never even know. For businesses, being hijacked in this way can result in significant losses. Customers will not come back and Google will penalize you in rankings or even delist you from searches. Thus, the hackers are targeting the business as well as their victims, or they simply do not care if you are harmed by their activities.

What kind of threats are out there?

There are a number of threats out there. One is 16shop, a phishing kit that targets Apple users. Most malware does not target Apple users, which can make them complacent about malware and phishing risks in general. 16shop tricks the user into thinking they are buying something from the Apple store, claims their account is locked, and redirects them to an "account verification" site that has a URL that looks legitimate, such as appleid dot com dot activity details dot info or apple-appleid.com dot customer-update-locked-service dot com. Note the com in the middle of the URL - that makes it much more likely that somebody will fail to notice the part afterwards, especially if they are using a short URL creator. The url will end in ?16shop. 16shop is mostly spread via email but is also an easily available phish kit. I was able to find two sites where we could download it...on the first page of Google.

16shop is so obscure, it is very hard to find information about this particular attack, despite the fact that it has been around for a year. Many users do not know it exists and thus are not alerted to protect themselves from it. It is basically a standard email phish, that shows an invoice for a purchase from

or through Apple. The email is designed to make you think you have been ripped off and panic. When you open the pdf, you will see a legitimate-looking email. The phishers want you to click on Cancel Order. Clicking any link will take you to a login screen that looks like the legitimate Apple site, but lacks the two page login Apple uses. It then asks for personal information and credit card numbers, then forwards you to Apple.com. You probably won't notice your entire identity is compromised right away.

How to detect if your site is infected

First of all, phish kits are clever beasts. They are often designed not to show up if you connect to the site from certain domains or with certain equipment. Shop16's Code, for example, indicates it has OS detection capabilities, and it may only show up for people connecting through macOS or iOS as a way of targeting their "customers" better. So, just loading your site may not spot the phish kit, even if it is replacing .index.php. If it is hiding under another URL, it can be even harder.

Step one is to do a quick scan of your website with a malware scanner. There are several free ones available. The scanner will look for files on your website that match known phish kits. You can also use it to spot anything you don't remember having put there. As phish kits generally block "threat" sites from loading them, looking at the files on your site is the only way. Also check your site for uploaded .zip files. Sometimes attackers get lazy and forget to delete the kit from your site after expanding it.

Also, if you find or are told your website is being flagged for malware, then you almost certainly have an exploit. It's a good idea to keep everything backed up, because sometimes the quickest way to fix a hacked website is simply to reinstall the entire thing. False positives do happen, but you should always run a full scan of your site if you have any indication it is being flagged.

How to prevent infection

The best way to prevent phish kits from being installed on your website is to run monitoring scripts that will alert you if anyone uploads files to your site. Also make sure you use a strong password for your website, and make sure the password is only given out to people who actually need it.

If you are using WordPress, then customize the admin login page to something completely non-intuitive. This customization reduces the risk of your admin password being brute forced. This is an example of how default installations often have vulnerabilities. Another example is the Apache banner, which shows anyone who visits the site the version number. You should turn this off, because it makes it easier for the hackers to spot vulnerabilities. Never use a default password. Two factor authentication is a very good idea for website admin accounts that have broad access to upload files and run scripts. Also, if you use WordPress, check that your theme is secure.

Keep your website patched and security software up to date. Run malware protection on every device used to access the site, including mobile phones. If you never update your website remotely, then turn that capability off. Install only the plugins, modules, and applications you need and promptly uninstall anything you are no longer using. Uninstall and replace plugins that are no longer supported.

Always educate yourself and your employees to prevent phishing attacks, as this might be one way hackers can get into your personal and business credentials, potentially endangering the security of your business and website.

Monitoring scripts can be hard to keep an eye on and waste time your IT people (or you, for very small businesses) could be spending on something more useful.