

Risk Professional - Business Crime - Google AdWords scam

Whilst the first "phishing" case we came across was back in the earliest days of PayPal, the vast majority of such scams use banks as their hook. But today we have received one purporting to come from Google's AdWords scheme. We show exactly how a phishing page is designed, explain the code to you and show why it works.

Google AdWords / AdSense are simply ubiquitous - it's seemingly impossible to open a webpage these days without their links appearing against often competing content.

And as it has become successful, it has become the vehicle for a number of frauds - including the infamous "clickfraud," a case Google settled recently.

And now the scheme is the victim of a "phishing" attack.

The following message is being distributed:

Please Update Your Billing Information.

Dear Advertiser, We were unable to process your payment.

Your ads will be suspended soon unless we can process your payment.

To prevent your ads from being suspended, please update your payment information.

Please sign into your account and update your payment information.

We look forward to providing you with the most effective advertising available.

Thank you for advertising with Google AdWords.

For those who have their email programs set to read text only (a very simple and sensible security approach) the message is relatively benign - after all, there is no fake link to click.

But for those who accept html (which Microsoft calls Rich Text), then the faking facilities of html mean that there is a link to a fake website.

This is how it works:

In html, to create a hyperlink, there is a simple command called "a." To link to an outside target, that is linked to command called "HREF."

The tag looks like this: `[description]`

You can try that for yourself: open a text editor (in Windows, that will be Notepad).

Copy the above tag and paste it into the Notepad window.

Change [address] to your company website address starting with the www. Don't repeat the http:// part.

Then change the [description] to "our website"

Click on File>Save as...

At the top of the box change the Save in.. to desktop (this is so you can find it easily later)

In File name - delete *.txt and type in "myfile.html"

The name before the dot is irrelevant. The extension after the dot tells your computer what type of file it is and what program to view it in. An html file is a webpage and the extension tells your computer to open it in a web browser.

In the "save as type " use the drop down box and choose "All files." This prevents Windows from adding a txt extension to the name you have chosen.

Click "save"

Now go to your desktop and find myfile.html.

Double click on it and it will open in a browser window.

As you can see, the only part of your code that is visible in your browser is the "mysite" that you put into the description section.

Click on that and the site for which you entered an address will open.

Go back.

When the page opens and you can see "mysite" again, go to the browser menu and click on View>Page Source (different browsers use slightly different words but their meaning will be clear.

As you can see, there is your code, the code you wrote in a text editor, saved as a webpage and opened in your browser.

It is the use of html in email that makes phishing easier by allowing the true target of the link to be hidden and also to allow the making of false letterhead with graphics, background colours and font faces that look like real letters.

In the Google AdWords scam, the visible link says "http://adwords.google.com/select/login" Therefore you would think that this is a real link. But the hidden link says ""

To read a web address, start at the back. When we do this, we get:

Login: this is the part of the website you will be taken to. Actually, its a file name with the extension removed because browsers know to look for certain file names and if the wrong extension is entered by a user, it will prevent the browser finding it. If the servers run on Linux with PHP, then the file will be login.php but if they are running a Microsoft server, then the extension will be .asp, .net or one or two others. As around 80% of the web runs on Linux, if people guess, they will usually guess php so writers often leave the extension off.

/select/ - this is a directory (folder in WinSpeak). It is where files are stored.

.cn This is not a file extension, it's a note of where the domain is registered. It's like .com which gives no geographical identity but in the case of .cn, it means China. However, the fact that a domain is registered in a particular country doesn't mean it is actually hosted on servers in that country.

sungroups - this is the domain name. To identify the owner of sungroups.cn you can try name search services. However, .cn names are very difficult to identify.

adwords.google.com. - in the real link, this is the address. In the fake link, this is a complex way of faking the address. Once you have reached the domain (in this case sungroups) every dot before that indicates a sub-domain. In some ways this operates like a directory but it has some special features. You don't need to know those - but you do need to know that when a browser starts to look for where to go, it reads the address just like the address on a proper letter. The .extension says which country, the domain says what business and the sub-domains say which floor of a virtual building to go to. This has multiple sub-domains so it's like saying which floor, which department and which desk.

The www is often not required - many domains are set up to be found without typing it in.

But not all are - for example you don't need to type in www to find any of our Group domains. But if you miss out the www in www.fsa.gov.uk, you will get a response that says the Financial Services Authority's website can't be found.