How to Avoid Hacked Websites

Don't Let a Website's Sloppiness Turn into Your Own Disaster!

This article shows you:

- Why hackers choose to target popular websites
- What you should do – and avoid doing! – after a website hack
- How to find out if hackers have infiltrated your accounts

Have you noticed that you receive fewer phishing scams by email than you did a few years ago? That's because criminals have moved on to bigger targets – and, sadly, easier ones: the websites themselves. Hardly a month goes by without our hearing that another website has been hacked and had all its customer information stolen. If you were one of those customers, how does that affect you? What should you do now? And could you have done anything differently before it happened? Read on to find the answers…

Contents:

Easy Prey: Why Hackers Target Websites ..... **H 585/2**
Prevent a Website Hack Becoming a Personal Disaster ..... **H 585/4**
What to Do if a Website You Use is Hacked ..... **H 585/5**
Have Your Own Details Been Stolen Already?..... **H 585/9**

Easy Prey: Why Hackers Target Websites

Website hacks have become common

In recent times, we've heard about successful hacking attacks on the websites of Sony, Wetherspoons, eBay, TalkTalk (three times), Ashley Madison and toy company VTech. There are undoubtedly a great many others: these attacks have become too frequent to keep up with, and attacks on less well-known companies won't be reported as widely as an attack on a high-profile website (if they're reported at all).

But when you read of a website having been hacked, what does that actually mean?

Websites at which you have an account

First of all, for our purposes, the websites that get hacked are those at which users have to set up an account, choosing a username and a password. (Other websites get hacked too, often with the purpose of planting malicious links or software, or defacing the pages in some way, but in these cases the motives and end results are different.)

The site stores your details in a database

When a customer sets up an account at a website, that customer's username and password are stored in a database on the site. This database is an ordinary computer file (you could create a similar database on your own PC), but it's not accessible to the website's visitors, for obvious reasons. Instead, when a visitor tries to log in by typing his username and password, those details are sent from the visitor's web browser to the website's server. The server (which is an ordinary computer, much like yours), checks whether this username and password appear in the database. If they do, the visitor is logged in.

You may have provided personal details too

Some websites ask for much more than just a username and password, and these details are also stored in the database as part of a 'record' for each customer. Some websites may ask for – and store – your date of birth,

postal address, phone number, and credit card details, among much else.

Your details should be encrypted…

Besides not being accessible to the website's visitors, this database should be protected in other ways. One of those is to encrypt the information it contains, such that if someone did get their hands on the data, it should be a stream of meaningless gobbledegook rather than a neat, easily-readable list of the customers' personal details.

… but very often they're not

This may sound foolproof, but it isn't. First, some methods of encryption are more secure than others, and – as many high-profile attacks have proved – not all companies pick an adequate method or use it correctly. Second, encryption might not be used for all the data. In some cases, while credit card numbers and passwords are encrypted, other details such as names, addresses and phone numbers are left as plain, readable text.

Hackers steal whatever data they can

This brings us to the initial question of why hackers target websites, and you've probably gone a long way towards answering it yourself. The hackers often won't know in advance what they're going to get (if anything), but in targeting a high-profile website they know they could get a haul of data about many thousands of people, and perhaps millions. The widespread carelessness about how data is protected means there's a good chance it won't all be encrypted, or it won't be encrypted very well.

It's sold, traded, and used for criminal purposes

From here, the hackers will usually publish the details freely online (usually in a hard-to-access portion of the Internet known as the 'dark web'), trade them or sell them. Anyone who gets their hands on a particular customer's data might then try using that customer's username and password at other websites (on the basis that many people use the same combination everywhere), or target that customer with email scams, or – if the haul included payment details – go on a

spending spree at that customer's expense, or attempt to steal their identity for other criminal purposes.

Not all hackers have criminal motives. Some are just children who regard it as an interesting challenge – an enjoyable diversion from gaming and Facebook. The security of some major websites has proved to be so woeful that no great skill or experience was needed to hack them.

Prevent a Website Hack Becoming a Personal Disaster

Can you be sure your details are secure?

Most of us have accounts at numerous websites. We don't know how well their databases are secured, or whether they encrypt all the various details we give them. We have to hope they're taking their responsibilities seriously – or better still, of course, that they never get hacked!

Take precautions

There's no knowing whether they will or not, so it's wise to take what precautions you can to limit the impact hackers could have on you. They're all fairly simple and well known, so I'll run through them quickly:

Use strong, unique passwords

- **Use a strong password** at any website which will store personal or financial details about you. Passwords should be encrypted in the site's database, but even so, a short or simple password could be easily decrypted by a hacker.
- **Don't use the same password** at any other website. If hackers do manage to get hold of your username and password, they'll try using that combination at other worthwhile websites.

Don't offer more than is needed

- **Try not to give any personal information** the site doesn't need. For example, a site should only need

your postal address for payment or delivery purposes, so if you won't be buying anything, a fictitious address would work just as well.

- **Invent answers to 'security questions'** such as date of birth, first school, mother's maiden name. As long as you keep a note of your answers, you can fulfil the requirements without giving away private details.

Use fictitious details

- **Have a separate credit card for online use** if possible – one with a low credit limit. The card company should always repay you for a hacker's spending spree, but that low limit takes away a lot of the worry while you wait for things to be settled.

Credit card with a low limit

It's not too late to apply these rules now!

Of course, the main targets for hackers are websites which might be expected to have financial details of their customers or a good store of personal information, and you probably have accounts at several such sites already. Even if you do, it's not too late to put some of the rules above to use: any website will allow you to change your password to something strong and unique if it wasn't already, and if your credit card details are stored, you can switch them to a different card. You may also be able to remove or change any personal details you've provided that the website doesn't really need.

What to Do if a Website You Use is Hacked

It's happened. One way or another, you've heard that a website at which you have an account has had its customer details stolen in a hacking attack.

How you hear of a website hack

How did you find out? Just possibly you received an email from the company itself, but that's unlikely at this early stage. Instead, you might have heard growing rumours online as other customers discovered their

accounts had been accessed by someone else and talked about it on discussion sites, or (most likely) you heard about it on the news.

Initially you won't know much…

At this stage, the details will probably be vague. No-one knows how many customers are affected (or, if they do, they're not yet saying), how much information was taken, or what this information is – whether it's login details, other personal details, or payment information.

… so assume the worst!

Right now, however, that doesn't matter: you always have to assume the worst. In other words, proceed on the assumption that anything the company knew about you is now in the hands of the hackers and being traded online. From here, follow these three rules:

Rule 1: Change any affected passwords

Change the password on this site…

If the website that was hacked is still up and running, log into it and change your password there. When you do this, make sure you really are going to the right website, either typing its address into your web browser's address box, or choosing it from your Favourites/Bookmarks list. Don't click links in any email messages you may have received.

… and anywhere else it's used

Did you use the same password for accounts at any other websites? If so, be sure to visit those sites and change their passwords too. Needless to say, don't set the same passwords for these that you've just set at the first website!

Rule 2: Keep an eye on bank and credit card accounts

Watch for unknown transactions

You don't know whether any payment details were stolen by the hackers, but if the website had those details you should assume they were included in the haul. Keep a close eye on your bank and credit card accounts, and contact your bank or card company straight away if you spot any transactions you don't recognise, however small they may be.

Note that fraudsters often try charging a very small amount to a credit or debit card first, aiming to find out whether the card is valid without raising suspicion, so don't ignore any seemingly-insignificant transactions – they may just be a precursor to something much larger.

Rule 3: Be ready for scam emails and phone calls

I mentioned earlier that you should always assume the worst once you learn that a website you use has been hacked, and this is the reason why. It doesn't matter whether or not any of your details were included in the haul: unless you're on your guard, the worst can still happen to you anyway!

Any user of the site could be targeted

Criminals who had nothing to do with the attack on the website have now heard about it, just as you have. They know that users of that website – like yourself – will be waiting nervously for news and advice. They know you'll be expecting an email or phone call from the company concerned at some point, and perhaps dreading a call from your bank about some sudden large payments you seem to have made.

As a user of that hacked website, you're a potential target for any fraudster out there, whether he has your details or not. With that in mind, remember that anyone who contacts you about this, however genuine they may seem, could be out to defraud you.

Contact could be made either by phone or email, and you should keep these tips in mind:

Be suspicious of email about the hack

Email: we're all used to receiving scam emails and you've probably learned to be sceptical. But when you're on tenterhooks waiting for news, you may be less suspicious. Nevertheless, the advice remains exactly the same as ever: not to click on links in email messages,

open attachments or follow instructions unless you have no doubt at all that the message really is genuine. In this situation, though, you might have to work a little harder at reminding yourself of this golden rule!

Scammers will telephone if they can

Phone calls: a scammer would love to telephone you, posing either as the website company or your bank. By contacting you this way, he can avoid giving you time to think or consult anyone, and he can get quick results. And however wary you are of email messages, you may well be more trusting of a phone call.

It's possible that your phone number was included in the haul of hacked data (or was traced using other hacked details such as your name and address). But it's equally possible that the scammer is just chancing his luck: with a high-profile hack like that of TalkTalk, for instance, with four million customers, a scammer could call people at random and he'd soon hit upon a TalkTalk customer.

Tricks to find extra information

If a scammer does telephone you posing as someone who works for the hacked company, the trick he'll use most frequently is to pretend that he has your details in front of him. He may even be able to quote some of them to you – part of your credit card number, perhaps, asking you then to confirm he's talking to the right person by reciting the rest of the card number or giving the security code on the back of the card. Several TalkTalk customers lost a lot of money by falling for this kind of scam call.

You should never have to prove who you are when someone phones you, and certainly not by quoting card details, bank account numbers or passwords. The caller can recite these details to you, and you can listen silently and then say whether or not they're correct. If he won't, for whatever reason, you must assume that's because he doesn't have them.

Alternatively, much as he would in an email message, he may try to give you instructions to follow – a website to visit, or a phone number you should call.

Make sure you know who you're talking to

Before giving out any information or taking any action, you need to know exactly who you're talking to. You know which company this person is calling from, so ask their name and which department they're in and tell them you'll look up the number of that company and call them back. (Again, any legitimate caller will be quite happy for you to do this.)

Make the call from a different phone line

This means you'll have to look up the company's phone number yourself (perhaps by returning to its website or using an online telephone directory), but that shouldn't be difficult. Having done that, use a different telephone line to make the call: if they called on your landline, for instance, use a mobile phone. You can then ask for the appropriate department and person.

It's important to use a different telephone line to make the call. A common scammer trick is to stay on the line after you hang up, preventing the call from ending. Thus, when you pick up the phone again to make the call a few minutes later, he's still there and he can pretend to answer the call, transfer you to the right department and carry on from where he left off.

Have Your Own Details Been Stolen Already?

Many hacks go unpublicised

Not all website hacks hit the headlines: wherever possible (and far more often than you might imagine) many companies will try to keep them quiet. Even for those you do get to hear about, you may have forgotten you ever had an account at that website, or the story

may die away without you hearing anything more, and you'll assume you weren't affected.

Are your details among them?

However, it's quite possible that your details were among the haul of a successful website hack and you were simply never told about it. If the company concerned didn't make it public or contact you, how would you know?

These websites can tell you

Well, there is a way. There are several websites which specialise in monitoring the chit-chat of the hacking community, gathering and collating the data that has been stolen and shared in website attacks. Since any haul of user details will contain email addresses at a minimum, these sites use email addresses as an indexing system: you visit one of the sites, enter your email address, and the results show you whether it has appeared in the haul from a website hack.

There are two popular websites of this type. The first will tell you where and when the hack took place, the other only the date of the hack:

www.haveibeenpwned.com

www.breachalarm.com

A free notification service

These two websites are more than just lookup services, however. At either, you can sign up for a free account and provide your email address, and you'll be added to a kind of 'watch list'. If your email address ever appears in a new haul of hacked data from another website attack, you'll receive an email alert from the service.

Early warning that your details have been hacked

If nothing else, these alerts tell you that you should quickly change your password at the hacked website, but they also forewarn you that other details you've provided at that site may now be in the hands of hackers. And, of course, all this is information you may not hear from the hacked website itself for days or weeks – if they ever tell you at all!