Two-Factor Authentication Explained

Online security should be important to everyone. From your email accounts to Facebook, if there's personal information on it there should be a password on it as well. But what if that's not enough?

If you've created an account online recently, be it for emails or Netflix, more often than not you'll be asked or even *forced* to add some form of Two Factor Authentication – a mobile number or second email address. As you are checking your emails for the inevitable verification link you're probably wondering "what's the point of all this hassle?"

The Problem

It is unreasonable to assume someone can remember several dozen unique usernames and passwords. However, a few reused passwords and another leak from Facebook later and suddenly you could have a serious problem on your hands.

IT experts are constantly looking for ways to improve security and one of the simplest ways of doing so is with Two Factor Authentication. By adding this extra layer hackers need to do much more than to crack the one password.

So how does it work?

As we mentioned before there are multiple ways to implement Two Factor Authentication. Most commonly you will be asked to supply a recovery email and maybe even a mobile number. In some cases, such as with your bank, you will need to download a mobile app to enable Two Factor Authentication.

The end result is similar: whenever you sign into your account after a long time or on a new machine you will be asked to verify your identity with a code sent to your smartphone. Now, if someone else is trying to sign in on another device there is no way for them to do so without your knowledge or permission.

But what if I don't have a smartphone?

Of course, not everyone will have a smartphone available which is why more often than not you will be offered several means of authentication: a regular text can be sent to any mobile and even some landlines, an email could be sent and read from the same machine, recovery questions can be answered from the same page.

Each website will have different options and requirements for what authentication can be set but more often than not it will be simple and easy to set up and use.

Now that I have Two Factor Authentication am I safe?

Not exactly. Whilst Two Factor Authentication will definitely bring a boost to your online security, no security measure is bulletproof. For example, a hacker could theoretically gain access to your recovery email or intercept your text messages and acquire the code for access. They might try to sign in from a trusted device without your knowledge or use social engineering to figure out your recovery questions.

All this is to say no one security measure will guarantee your protection. However, for how simple it is to implement Two Factor Authentication remains highly effective in protecting your accounts and along with a sensible approach to online security it should protect you from a majority of hacking attempts.

If you want to check which of your passwords are available online visit https://www.keepersecurity.com/en_GB/free-data-breach-scan.html **to see if you have been involved in a data breach.**

If you are concerned with your online security and would like advice, give our engineers a call on 01604 411444

Is your computer slowing you down and making it hard to work from home? Is your PC too old to make videocalls? Call us today to arrange your computer upgrade today on **01604 411444**