What to do if you are breached.

Email fraud is on the rise, and SMB's are suffering at the hands of these fraudsters every day. If you are one of these companies, here are the steps we recommend you take and the steps we take for you. Make sure you familiarise both yourself, and all your employees on these steps. They aren't complicated, but having a process in a tense situation keeps things moving in the right direction.

If you/a member of your staff have "clicked on a link" that you feel suspicious of, then -

Step one: Call us.

Not in 10 minutes once you have discussed it with colleagues, not even once you finish reading this first step. Call us the moment you suspect something has gone wrong. The call should only last a couple minutes, and we will start to stop further actions immediately. **Note:** We may tell you to turn off your PC's and disconnect from the internet cables depending on the type of link you describe, so please give us as much information as possible.

Step Two: Cut off payments.

If there's been a bank transfer that you have instigated, contact your financial institutions and stop all outgoing payments from your accounts. If it is a 3rd party or a client, inform them to do this ASAP.

Step Three: Notify your team.

Send an internal email to your team or a group message for them all to change passwords and to suspend out-going payments until you know it is safe to do so.

Step Four: Prevent it from happening again.

Once you have received the relevant information from us, you must then make sure this kind of breach doesn't occur again. We can book in a security audit/meeting with yourself; there are very cost-effective tech options that can prevent these at the click of a button. There are also manual, and straightforward methods of doing this. Have staff regularly change passwords, regular email rule audits and internal training. Though these are free to do, they do require quite a lot of time and management to enforce across your company, often with the tech alternative outweighing the risk & time.

LUCIDICA

The IT team for your business

What we will do.

Step one: Stop the breach.

We will work as long as it takes to stop the violation from continuing and remove the fraudster from the system that they have infiltrated. We follow an official security breach incident management process to ensure we're covering all bases.

Step Two: Investigate.

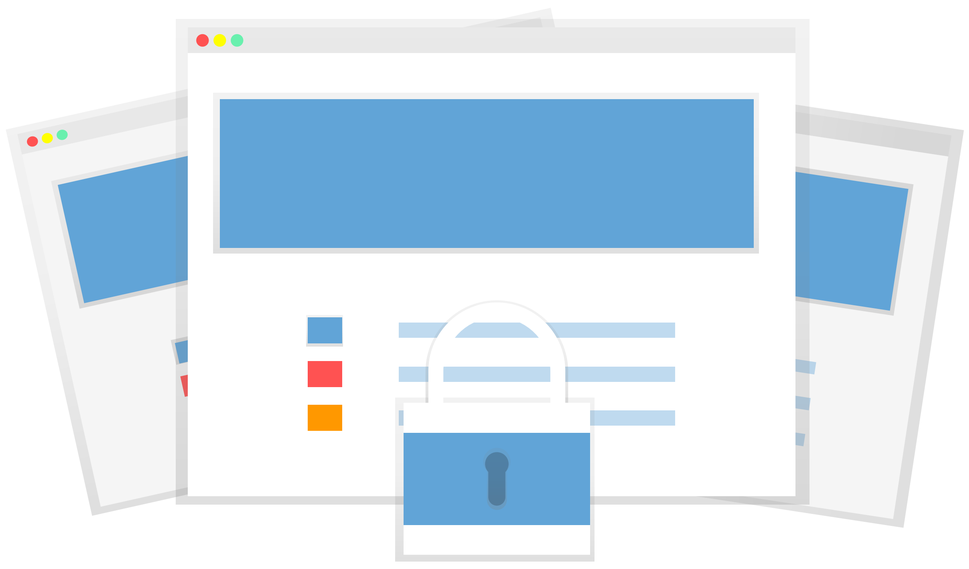
If you are on one of our MCS Security Packages, you will have a set amount of time included within your charge under 'Incident Management'. This time can range from 6hrs to 24hrs, where we will investigate and provide advice and solutions.

If you are not under one of our MCS Security packages, we will spend up to an hour producing a basic report for you. The report will include what has happened, who it has affected and what we recommend going forward.

Step Three: Full incident report & clean-up.

Dependent on the complexity of the incident depends on the time it takes to do a deep dive and clean-up, its is down to you whether this is something you see are required, but we do recommend it after every incident.

Not only will we clean-up the potential mess left behind by fraudsters but we will also do a company-wide scan of inbox's for malicious activity, reset passwords and permissions and provide relevant advice regarding best steps to prevent future attacks.



To read more on Business Email Compromise, the current most common and efficient fraud seen in the SMB market, read our educational blog on our blog site.

www.Lucidica.co.uk/blog/recent-news

LUCIDICA

The IT team for your business