Bates Wells

TOP TIPS IF YOU'VE HAD YOUR EMAIL HACKED

A Charity's Guide

Certified B Corporation

www.bateswells.co.uk

Introduction

It's a shame we had to write this guide. But unfortunately hacking, phishing and other blagging attacks are becoming more and more common – particularly in a work context.

Whether it's your email that's been hacked or whether you've received an email from a hacked account, you will want to know how to protect yourself and your charity.

We consider the damaging effects of email hacks from every legal angle. So we have explained below what you should do if you find yourself in this position.

#1 Minimise any further damage

Before you assess the damage done you should act quickly to minimise any further damage to yourself or others.

We suggest you:

- **Change your password immediately** – this will keep the hackers out of your account. Switch on two-step verification and update your security questions, if these options are available.
- **Check your settings** – sometimes hackers change your contact details or settings so that they can continue to access your account.
- **Tell your contacts and colleagues that your email has been hacked.** Ask them to delete any suspicious looking emails from you without clicking on any of the links.

#2 Speak to your IT team – or another IT professional – to assess the extent of the hack

You will need an IT professional to assess the hack and consider whether you will need to remove any malware from your devices or your systems. They will be able to determine what has been accessed and when.

You will need to take the appropriate action to contain any breach and recover, rectify or delete the data that has been lost, damaged or disclosed.

#3 Notify your insurers

You should notify your insurers at an early stage. This applies when you might need to make a claim - but also if the hack might lead to a claim against you. If you have cyber insurance, your insurers will be able to assist in a remediation plan.

#4 Consider your obligations

You should consider which regulators you are required to disclose the hack to. You may need to report the matter to more than one regulator, beyond the two we've listed here.

Information Commissioner's Office (ICO)
You should inform the person at your organisation who is responsible for data protection. They'll need to consider whether the matter should be reported to the Information Commissioner's Office. If the matter does need to be reported to the ICO and your organisation is a controller, you'll have 72 hours from becoming aware of the incident to make the report. If your organisation is acting as a processor where data has been hacked, you should inform the relevant controller(s) immediately regardless of whether you think the incident should be reported to the ICO.

Charity Commission – serious incident report

If your organisation is a charity, you'll have additional regulatory obligations. The email hack may require you to report a serious incident to the Charity Commission if it results or risks significant:

- harm to your beneficiaries, staff or volunteers
- loss to your charity's money or assets
- damage to your charity's property
- harm to your charity's work or reputation.

It is your trustees' responsibility to decide whether the breach is significant and should be reported.

We suggest you:

- consult with your trustees immediately
- consider the Charity Commission's guidance at **www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity**
- speak to your solicitors for advice on whether the hack needs to be reported
- include in your report details of steps you have taken to mitigate the impact of the hack and minimise the risk of another one.

#5 Consider whether to make a claim for compensation

Once you have established the impact of the hack you will want to consider whether you can obtain compensation for the data security breach. Your data may have been stolen because another company's security systems are inadequate. There is a right under data protection law to receive compensation if a person has suffered damage as a result of an infringement of the law by another party. However, you should also check any contract your organisation has with the party responsible for your security systems since this may set out limits on liability for claims.

We suggest you:

- Preserve the evidence related to the hack and how it happened
- Consider the likely value of a claim for compensation – what are your losses?
- Consider who might be liable and why
- Speak to your solicitors for advice on how successful a claim is likely to be.

#6 Put a documented plan in place for dealing with future data security breaches

If you do not have a policy in place that deals with addressing a data security breach, including notifying authorities, it would be a good time to develop one.

There's also lots of guidance available from the National Cyber Security Centre: **https://www.ncsc.gov.uk.**

We suggest you:

- Develop and policy and plan for dealing with future email hack and data security breaches
- Consider training for your staff to ensure they're equipped to prevent and manage future data security breaches.

Our solicitors are experienced in acting quickly to manage situations just like this.

Contacts

Robert Oakley
Partner, Counter-Fraud and Dispute Resolution
020 7551 7792

Eleonor Duhs
Partner & Head of Data Privacy
020 7551 7929

Mindy Jhittay
Senior Associate, Counter-Fraud
and Dispute Resolution
020 7551 7853

fightingfraud@bateswells.co.uk

Bates Wells

Making a profit is core to all businesses but our goal is to combine this with a real social purpose. Our values are important to us, they shape our decisions and our working life.

Since opening in 1970, we've focused on positive social impact as much as we have on being a successful law firm and we were the first UK law firm to achieve B Corp certification.

Today, our clients are diverse – from corporate household names, to public bodies, to start-ups. We're also the firm of choice for thousands of charities and social enterprises. We continue to lead the market we helped to shape.

As a purpose and values driven firm we show commitment to our clients, our people, the environment and society. We see it as our purpose to create a positive impact. The impact we have on our people, our communities and our planet does more than inform our work – it gets us up in the morning.

Bates Wells challenges what is possible in legal expertise delivery.

Get in touch:
+44(0)20 7551 7777
hello@bateswells.co.uk

www.bateswells.co.uk