After Lockdown: Bates Wells Guide

To to tackling fraud

For all of us, the coronavirus (COVID-19) pandemic has been a time of dramatic, unprecedented change to the way we live and work. Sadly, the more things change, the more some things stay the same, and fraudsters have already begun to use the pandemic – and the associated "lockdown" - as an opportunity for new scams.

Scams to watch out for

Many scams rely on social engineering, a form of psychological manipulation designed to mislead your people into performing actions or divulging information which allows fraudsters to gather data or access your computer system. As this exploits human error, people are naturally more vulnerable to it at times of stress, uncertainty and anxiety – going into lockdown, or starting to come out of it - when they are more likely to panic in response to an unsolicited, and often unwelcome, email or text.

Scams will often include the following elements:

1. **Impersonation** – e.g. an email that looks like it comes from someone/thing important to you or your charity
2. **Intent** – this could be a "lure" like a promise of payment or a "threat" such as lifesaving coronavirus protection information in an attached document or link. There is also usually an element of time pressure.
3. **Payload** – the email/text will likely include a seemingly inconspicuous link or file that will, for example, enable the fraudster to gain access to your computer if clicked/downloaded.

During the COVID-19 pandemic, scams employed by fraudsters have included:

- Text messages, claiming to be from the government, which direct people to an imitation of the government website where they are prompted to enter their personal and card details in order to receive a "COVID-19 relief" payment;
- Clone firms', which impersonate firms registered to do things like sell, promote, or advise on the sale of insurance products or pretend to be one of your current suppliers/beneficiaries;
- Communications from fraudsters impersonating claims management companies claiming to be able to help recuperate losses caused by (for example) event cancellations;
- Emails, calls and texts from someone claiming to be from your bank, who takes advantage of the financial uncertainty created by the coronavirus to convince you to transfer your money to a new bank or promote non-standard investments;

Top tips for fraud prevention

You can protect your charity against fraud by keeping in mind the following tips:

- **Sense-check** – Where you expecting the email? Run unfamiliar requests past colleagues for a common-sense check. If the email is supposedly from (for example) a supplier or beneficiary, check with them using the contact details you have on record. If an unfamiliar communication claims to come from a provider of financial services, check their credentials using the Financial Services Register.
  Never reply directly to the email/text and never click on the link or open the attachment if you have concerns.
- **Review your policies and procedures** - Make sure that your normal processes for fraud prevention, such as dual authorisation and the monitoring of financial transactions, are resilient and can continue to function in the event of disruption. Remind staff of the need to follow these processes, even in unusual working conditions. It may also be helpful to agree an "I will never" list for your organisation to help staff identify fake internal communications.
- **Implement security basics** - make sure virus protection, unique user IDs and passwords and restrictions on access to online payment systems and other sensitive information are reliable even if your organisation is largely or wholly working from home.
- **Report it** – the most important thing you can do to protect your organisation and others is to report anything suspicious as soon as possible. This helps to identify new and emerging scams and issue warnings and alerts where appropriate. You can report to the Charity Commission, Action Fraud, the Suspicious Email Reporting Service, or your Bank/other regulators/funders as appropriate.
- **Stay vigilant and don't panic** - Above all, stay vigilant and stay calm. Do not act if you're feeling panicked or unsure about an unfamiliar communication, even (and especially) if you're being told to act urgently.

For more advice, please get in touch with our Counter-Fraud team:

Robert Oakley
Partner
T: +44 (0)20 7551 7792
E: r.oakley@bateswells.co.uk

Mindy Jhittay
Senior Associate
T: +44 (0)20 7551 7853
E: m.jhittay@bateswells.co.uk