The Coronavirus scams you need to avoid

URGENT
ADVISORY
URGENT

Urgent advisory, issued by Dial A Geek on 24 April 2020

These uncertain times are bringing about a real global sense of community.

However, while most people are helping friends, family, and even strangers, some unscrupulous scumbags are taking advantage of the crisis for their own benefit.

Cyber criminals are using more and more sophisticated methods of conning decent people. Consumers and business owners & managers.

Some of the new tactics being used at the moment are frightening.

There are new tricks being used, and some are extremely convincing. We've issued this urgent advisory so you don't make it easy for them to trick you out of your money and personal data.

This is not intended to be a comprehensive guide, just an up-to-date overview.

Scams

Everything you've been told about phishing emails in the past still applies now. We're also seeing a surge in the number of scam calls being made to businesses and households. These are a few examples of what to look out for:

- Emails or calls inviting you to invest in in-demand industries, such as pharmaceuticals, or 'safe havens' like gold and oil. Alternatively, you may be advised to transfer existing investments due to the uncertain stock market.

- You may be asked to invest in good causes during this time, with the promise of high returns. Rarely are these genuine, so steer clear. It's highly unlikely that a genuine request for a donation will arrive in your inbox (or to your phone), and donations don't come with the promise of a return on your investment.

- Loan offers with an upfront fee. You'll be offered a loan, whereby you pay an initial fee (something between £25 and £450 is common) and you get to borrow the sum you need. But after you pay this fee the loan never materialises and the 'company' disappears. Avoid them!

If you're concerned about money, speak to your bank as a first port of call. They'll be able to take you through your options and help you decide which is best for you.

- Calls or emails from so-called health professionals, requesting your personal information and/or card details. Fortunately, in the UK we're covered by the NHS for treatment, but if you have health cover like BUPA for example, you may be tempted to fall for this. Always call them back using the number on your paperwork before you give away any information.

- Calls from Claims Management Companies, insurance companies, or your "credit card provider". Perhaps you've had to cancel a holiday, or even a wedding. These calls will promise to re-cover your losses on your behalf. They'll ask you for bank details or for a fee. Do not give them anything.

If you need to make a claim with your credit card company, go directly to them. If you have insurance, go directly to them. Do not entertain the offer of help from a cold caller.

- 'Clone' emails or calls. The emails or calls claiming to be from a genuine, reputable company, but are actually just good fakes. They may look the real deal, but they'll be asking for a reply containing some of your personal details, or for you to log in to their webpage to update your information.

Don't click links if you're unsure that the sender is genuine; and don't ever give out personal information if you're unsure. Do your homework, check the email address it's been sent from, check the spelling and grammar in the message. Look at how they've addressed you in the email - is it Dear Sir, or Dear Mr John Jones? If you're still not sure, contact the company directly using the number on your paperwork or their website.

Online and emails

You may have been receiving more emails than usual lately. Your regular subscription list may be offering 20% off here and free delivery there, but emails with offers that seem just too good to be true are on the rise.

Remember, if something seems too good to be true, it usually is.

- If it's an email, check the sender's address. Does it look genuine?
- Check the company's website. Does it have the same offer online?
- Check the spelling and grammar. Is it the same style that the brand usually uses?

Do not click on links if you're at all unsure whether they're genuine or not.

Clicking a dodgy link can lead to malware being placed on your computer. That gives cyber criminals access to your personal information and can lead to all manner of losses on your part. Your money, your accounts, even your identity.

You're probably using social media a lot more at the moment. While social media can be good for connecting with friends and family, be careful what you post.

Cyber criminals utilise social media in a big way and will think nothing of targeting a potential victim and scrolling through their social media accounts to uncover the personal information they want. And sadly, it's not that difficult to discover a lot about you if you use social media regularly.

For example, you may have seen lots of 'getting to know you' quizzes lately on Facebook. Scammers can and do use your answers to those to capture your information. First pet? First car? Do these sound familiar as some of your memorable questions? **Avoid them.**

Passwords

We really can't stress this enough: Use long, randomly generated passwords to make them really difficult to crack. Using your child's name and date of birth is no good (think back to social media, if you've posted photos of their birthday cake, James010317 is not a good password!).

Pro tip: **think of a sentence and take the first letter of each word to make up your password. For example, 'Clicking one dodgy link could risk your personal data' would make C1dlcrypd. Now you have a memorable, difficult to hack password.**

Better still to randomly generate passwords, and use a password manager to remember them for you.

Staying safe is easier when you stay vigilant

Times like these call for extra vigilance. Sadly, some people are more devious than we'd like to imagine, and this pandemic is a goldmine for them.

Take care and pay extra attention with communications from companies and strangers. And you won't fall into their trap.

We're Dial A Geek, and we support lots of Bristol businesses with their IT.

If you're unsure whether something is to be trusted or not, contact us and we'll help you decide. If you need any other help or advice with your technology or data security, **let's talk.**

How to contact us:

- Hit the 'reply' button to email the office
- Email the Geeks: help@dialageek.co.uk
- Dial A Geek: 0117 369 4335

DIAL A GEEK