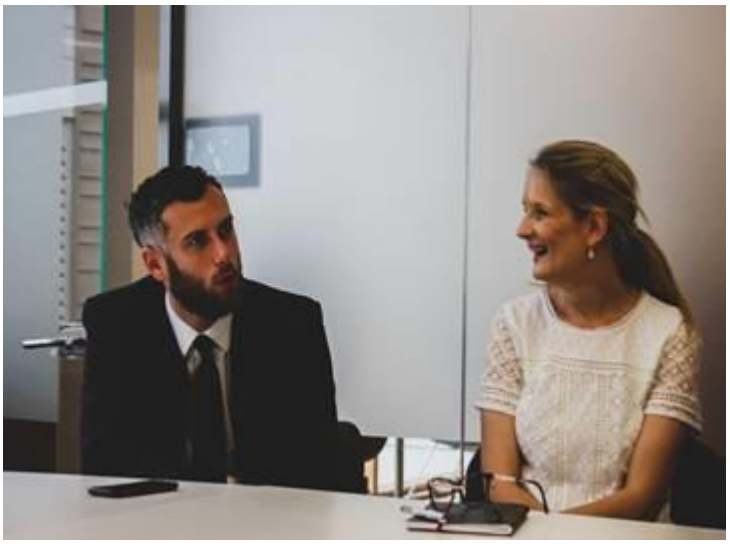
View this email in your browser

www.onewest.co.uk

Important - Please pass to your Business Manager & share with staff

An update from Sean Smythe – One West Information Governance expert

COVID-19 Cyber Scams to continue to watch out for



Not all of you will have met me. I'm **Sean Smythe** and I head up **Information Governance** in One West.

Part of my role is keeping up to date on what's happening in the world of **Cyber Fraud.**

Unfortunately even now some people **continue** to attempt to benefit from COVID-19 by **scamming** others.

In researching what is **'out there'** at the moment I still find it quite amazing how many scams there are & how vigilant we need to be!

There is no doubt that as different things hit the news even beyond COVID-19 this sort of thing will **continue**. Scams aren't only directed to us in **work** but also in our **home** lives.

In my mind that means we need to adopt an approach which is **active** in identifying arising scams & letting each other know when we become aware of something problematic **wherever** this comes from.

If the fraudsters keep getting found out it can do a lot to slow them down but of course they will find **other ways** so all of us need to think more broadly & make sure we are secure in all aspects of our IT.

It is an area we can **help** with – we work with customers to check out their cyber security resilience which in turn gives **reassurance** to them that they are doing all they can to avoid issues.

If you are interested in **knowing more** just ask via one_west@bathnes.gov.uk

Scams to look out for **right now** are:

- **Re. Free Tesco Vouchers**. This includes a link to a (spoof) website where recipients can register to claim 'vouchers' - in the process victims divulge email logins and personal details.
- **Re. COVID-19 Government Grants.** Scammers claim to be from the 'UK Business Advice Bureau' offering grants up to £25,000. The victim must enter further details to gain more information about the scheme.
- **Re. World Health Organisation (WHO) grants/compensation.** This claims the victim has been selected to receive a grant worth $15,000 or a compensation payment of $500,000. Victims must contact a 'payment department' and provide them with their personal details in order to progress.
- **Re. COVID-19 rapid testing kits.** Scammers claim to be from a business called 'Clarity Medical Healthcare' selling rapid testing kits for COVID-19. The emails link to a (bogus) website were victims can enter their details to 'pre-order'
- **Re. Virgin Media.** Victims are advised to click on a link to view their bill. The email looks fairly legitimate, however minor details such as billing amount are incorrect (it's often stated as '£60.78') Other emails claim to be from the 'e-

billing team' and advise that the victim's account is frozen as their bank details cannot be validated. Again, these emails look 'normal'. They feature a link to 're-validate or amend billing details' (which provides fraudsters with the opportunity to steal their email passwords and personal details.)

- **Online shopping fraud.** Beware of the many bogus websites claiming to sell face masks, hand sanitiser, loo rolls, 'immunity gels' and COVID-19 testing kits etc.
- **Donation requests.** These come via email/text from 'charities' marketing themselves as helping the vulnerable during the pandemic.
- **Bogus banking calls.** Callers claim bank accounts have had unusual activity or been compromised. Victims are pressurised into giving away password/PIN details and/or setting up a new (fake) account. Victims have also been advised not to visit and/or contact their normal bank branch due to the pandemic.
- **Rental property scams**. This is where victims are persuaded into making advanced payments against rental properties that they have not seen due to COVID-19, and (in most cases) do not even exist.
- **Financial assistance fraud**. This comes via email/social media where scammers pose as a friend of the victim and use COVID-19 as a reason to request financial assistance from them. Victims believe they are helping a friend.
- **Pet adoption scams.** Animals are offered for sale and sellers use COVID-19 as an excuse for victims not being able to see the animal in person. Victims are persuaded into making advanced payments to secure the animal, which is subsequently never provided to them.
- **Automated messages.** These claim to be from the Government advising that all individuals must now wear a face mask in public. Victims are given a number to call to make an order.
- **Emails urging investment.** These are especially in (bogus) bitcoin schemes.
- **Emails directing download.** These are of a 'live map' of coronavirus cases. The download is in fact malware which infects the victim's device and attempts to gain unauthorised access to their network.
- **Courier Fraud**. This is where victims receive an unexpected phone call claiming to be their bank or even the Police. The caller advises of an issue with the victim's card and asks for their PIN & address details. A 'courier' then arrives at their address to collect the victim's card.
- '**Smishing' texts spoofing HMRC.** These are texts claim to be from HMRC advising victims of potential tax rebates. They link to a (fake) website where

the victim must enter their details in order to see if they are ‘eligible’. (Here’s more info.)

I must say in this bewildering array - if the worst happens and you click a link don’t panic!

What you might need to do is to ensure you change your password and report it to your IT provider ASAP.

If you would like further advice on Cyber Security don’t hesitate to drop us a line: One_West@bathnes.gov.uk

Our continued best wishes whilst the Lockdown eases.

Regards

Sean

Our mailing address is:

One_West@bathnes.gov.uk