Cornwall Council Audit Services

Fraud Awareness Alert for Schools
Alert 36 – March 2020

Cornwall Council receives intelligence related communications from national and local organisations which provide information about possible fraud risks that may affect Council Services, schools, employees and members of the public.

It is hard to believe that even at this unprecedent time fraudsters continue to operate, and worse than this in some cases they are attempting to exploit organisations, and the public at large, through scams linked to the coronavirus pandemic.

The purpose of this alert is to highlight some of the current scams, the majority of which have been reported by the Chartered Trading Standards Institute (CTSI).

School Meals Scam

We are aware of a large number of cases where parents are being contacted about school meal provision.

The fraudster requests the parent to provide bank account details in order to retain a free school meal entitlement.

For example, some parents have received emails stating:

'As schools will be closing, if you're entitled to free school meals, please send your bank details and we'll make sure you're supported'.

The Department for Education has urged anyone receiving such emails not to respond to them and to delete them immediately.

Bogus Healthcare Workers

CTSI has warned the public not to open their doors to bogus healthcare workers claiming to be offering 'home-testing' for the COVID-19 Coronavirus.

Suspicious callers are said to have been knocking on doors of elderly and vulnerable residents in various parts of the UK, saying that they are health officials doing door-to-door testing.

Katherine Hart, CTSI Joint Lead Officer for Doorstep Crime, has commented: "There are unfortunately people who are willing to take advantage of those who are most vulnerable even at this unprecedented time when we should all be pulling together. Those who have been advised to avoid social contact as part of the measures to help stop the spread of the virus are particularly at risk of being taken in by these cold callers. Our message is not to open the door to anyone you don't know or anyone calling 'out of the blue'. Stay safe by only speaking to people you know and trust."

Tax Rebates

CTSI have also reported the existence of scam emails claiming to be from the Government, offering tax rebates to support people through this challenging period.

The emails, which look official, inform the recipient of the rebate amount and request that they click a link to receive it. At the link, the recipient is asked to fill in personal details, including their credit card number and address. These details allow the scammer to take money directly from the recipient's bank account.

World Health Organisation

Fake emails purporting to be from the World Health Organisation (WHO) have been identified.

The emails, which claim to hold crucial coronavirus safety advice, have an attachment which if clicked on downloads a "keylogger".

"Keyloggers" allow scammers to follow the online movements of the user, and by doing this the fraudster can gain access to the device; the user's passwords; personal details and other confidential information.

Fake Phone Apps

CTSI have advised the public to be wary of an emerging scam involving fake phone apps.

There are reports of several 'coronavirus update' apps, which claim to provide updates on the virus. The fake app contains a form of 'ransomware', named "CovidLock", which upon downloading, locks the phone and displays a message demanding that the user pays a

sum of money to unlock it. These apps are available to download from various unofficial websites.

Phone users are advised to only download apps directly from the Apple Store, or Android Play Store as these are safety checked by the platforms.

Repair Work Opportunists

CTSI has issued advice to the public on utility and emergency repair work being performed during the coronavirus pandemic. They have been made aware of opportunists trawling social media for individuals looking for emergency repair work at this increasingly difficult time.

CTSI advise individuals to ensure that for any emergency work, the price is agreed on upfront; the agreement is put in writing and is with a trusted trader, or one you've used before. They add:

"We are aware of unscrupulous businesses who are trawling through social media and preying on people at this time of crisis, offering to do work that is substandard, unsafe and at grossly inflated prices. Any non-emergency work still needs to comply with cancellation regulations and a cooling-off period. If it is a non-emergency, please wait until this crisis is over. Do not put your family at risk by using someone that you don't know."

Text Scam

CTSI has been sent evidence of a text scam that is circulating which claims to offer a lump sum payment from the Government to the recipient.

Similar to the recent email-based scam offering a bogus tax rebate from HMRC, this new scam claims that the Government are offering lump-sum payments "as part of its promise to battle COVID-19”. Each text specifies a particular sum and asks the recipient to tap the link to what is a bogus website which requests payment details from the recipient.

CTSI state:

"The government are not issuing lump-sum payments, and anyone who receives these texts should ignore them and not tap the link”.

Bogus Fines for Breaking Lockdown

CTSI report a new text scam purporting to be from the Government informing the recipient that they have been issued with a fine for leaving the house during the lockdown.

The message claims that the movements of the recipient are monitored through their phone and they must pay a fine.

The distressing texts are entirely fraudulent and are an attempt by scammers to steal the credit card details of text recipients.

CTSI comment "We see new scams daily, and I would urge people to seek advice before replying to any messages they receive. This latest text scam issues a fake fine which tells the recipient to pay a fine or face more severe action. Anyone who receives this text should ignore it. It is simply another ruse to steal the payment details of users. In all of these cases, do not click, or tap any links that these messages ask you to."

Online Shopping

Action Fraud have advised that they have received numerous reports relating to on-line shopping scams, where people have ordered and paid for items such as protective face-masks and hand sanitisers which never arrive.

The following advice is given to protect yourself from becoming a victim of such fraud:

- Make sure you've installed the latest software & app updates. Criminals use weaknesses in software to attack your devices and steal information, such as your payment details.

- Use a strong, separate password for your email account. Criminals can use your email to access other online accounts, such as those you use for online shopping.

- Don't click on a link in an unexpected email or text.

- Don't pay for goods or services by bank transfer unless you know and trust the person. Payments via bank transfer offer you no protection if you become a victim of fraud.

- Be careful when using direct banking transactions to pay for goods. Make sure transactions are secure.

- Don’t send confidential personal or financial information by email.

- Use an online payment option such as PayPal, which helps to protect you, or use a credit card if you have one, as most major credit card providers insure online purchases.

- If you are using a retailer for the first time, always take time to research them before you give them any of your details. Be prepared to ask questions before buying.

- Trust your instincts – if an offer looks too good to believe then there is usually a catch. Be suspicious of prices that are too good to be true.

- Be sure you know who you are dealing with. Always access the website you are planning to buy from by typing the address into your web browser and be extremely wary of clicking on links in unsolicited emails.

- Only use retailers you trust, for example ones you know or have been recommended to you. If you’re buying an item made by a major brand, you can often find a list of authorised sellers on their official website.

- Whenever you are typing in personal information, make sure that the web address (in the address bar) begins with https (the s stands for ’secure’). Also check to see if a small locked padlock appears in the browser window. The ’padlock’ is one way of checking that a website is secure and indicates that your information will be encrypted.

For more information on how to shop online safely, please visit: https://www.actionfraud.police.uk/shoponlinesafely

Phishing Emails

Action Fraud have received hundreds of reports of coronavirus-themed phishing emails. These attempt to trick people into opening malicious attachments which could lead to fraudsters stealing personal information, email logins, passwords and banking details.

As mentioned in previous alerts, bogus communications sent by scammers are often designed to appear to come from trustworthy enterprises and may contain malicious attachments or website links in an effort to infect computers or mobile devices.

The communications will often ask you to click on a link, or open an attachment, which can then infect the device you are using with a virus, often designed for fraudulent purposes, or to aid other illicit activity. Such viruses can have extremely serious results.

Please note that the following should always ring alarm bells:

- Unexpected emails or other communications that ask you to click on an external link (even if you know the sender, their mailbox may have been hijacked)
- Emails from people or organisations you do know, but where the content seems out of character or out of place (the email address that appears in the 'from' field of an email is not a guarantee that the email came from the person or organisation that it claims to have originated from)
- Misspelled domain names or email addresses made to look very similar to legitimate ones, for example cormwall.gov.uk; cornwwall.gov.uk; cornwall.govv.uk
- Unexpected attachments from external sources
- Strange or unusual content that indicates you must take quick action to gain a reward or to avoid a negative consequence
- Web hyperlinks which display something different to the link itself when your mouse is hovered over it
- Emails asking for your password, PIN or other credentials
- Emails containing odd 'spe11ings' or 'cApitALs in the 'subject' box and/or spelling or grammatical errors in the content of the email (this is often an attempt to get around spam filters and into your inbox)
- Fraudsters are unlikely to know your real name, so the email may address you in vague terms, for example 'Dear Valued Customer'

If you receive any suspicious emails delete them. Do not reply to them, click on any embedded links within them or open any attachments that they contain.

Please remember that as well as email, text messaging, social media such Facebook and Twitter and instant messenger chats, like Skype can also be used to distribute malware, so exert the same diligence in your use of these channels.

If you ever mistakenly open an attachment, or click on a link in a suspect email, always report it immediately to your IT Provider.

Amazon Prime

This scam is not linked to the coronavirus pandemic, but involves victims receiving an automated call, informing them that they have been charged for an Amazon Prime subscription.

They are subsequently instructed to 'press 1' to cancel the transaction. When they do this, they are directed to a fraudster posing as an Amazon Customer Service Representative.

The fraudster advises the victim that their subscription was purchased fraudulently and that remote access to their computer is required in order to fix a security flaw that will prevent it from reoccurring.

The victim is asked to download a remote access application, often the 'Team Viewer' app, which grants the fraudster access to their computer.

The Team Viewer software is then mis-used by the criminal to monitor the victim logging onto their online bank account, which allows the fraudster to see the victim's personal and financial details.

Other variants of the crime involve fraudsters stating that the recipient is eligible for a refund for an unauthorised transaction on their Amazon account.

Take steps to protect yourself:

- Always question uninvited approaches in case it is a scam. Instead, contact the company directly using a known email or phone number.

- Have the confidence to refuse unusual requests for personal or financial information. It's easy to feel embarrassed when faced with unexpected or complex conversations. But it's fine to stop the discussion if you do not feel in control of it.

- Never install any software or visit a website as a result of a cold call. Unsolicited requests for remote access to your computer should always raise a red flag.

Fake PayPal Emails

Action Fraud is warning people selling items online to be on the lookout for fraudsters sending fake PayPal emails.

Fraudsters will send the victim an email purporting to be from PayPal, in attempt to trick them into believing they have received payment for an item.

The fraudster will then send a follow-up email requesting a tracking number in the hope that the victim will be rushed into shipping the item before they have had a chance to verify the payment.

Director of Action Fraud, Pauline Smith, said:

"We know that fraudsters will go to great lengths to target people on online marketplaces, which is why we are working hard together with our partners to highlight the threat and prevent people from falling victim.

It's really important to follow our advice to help protect yourself and always trust your instincts – criminals will try and make unusual behaviour, like asking for a tracking number before you have sent the item, seem like a legitimate request.

If you think you have been a victim of fraud, please report it to us."

A spokesperson for eBay, said:

"Millions of buyers and sellers use our marketplace safely each day around the world. eBay takes privacy and security extremely seriously, which is why we continually invest heavily in measures to protect users around the clock. We also work closely with law enforcement agencies and regulatory bodies.

Fraudsters use very sophisticated methods to try and circumvent trusted website security and we continuously enhance and update our security infrastructure to tackle new fraud trends. We encourage all members to take precautions that will improve the level of security protection on their accounts.

Don't get caught by fake payment emails and always confirm you've received a PayPal payment before sending an item – check your PayPal account and ensure the payment icon in your My eBay is highlighted. For more information and suggestions, check our guide to avoiding payment problems on the eBay Customer Service page: https://www.ebay.co.uk/help/home"

- **Sellers beware**: If you're selling items on an online marketplace, such as eBay, be aware of the warning signs that your buyer is a scammer. Don't be persuaded into sending anything until you can verify you've received the payment.

- **Scam messages**: Don't click on the links or attachments in suspicious emails, and never respond to messages that ask for your personal or financial details.
- **Listen to your instincts**: If something feels wrong then it is usually right to question it.

PayPal offer the following advice:

"At PayPal we go to great lengths to protect our customers in the UK, but there are still a few, simple precautions we should all take to avoids scams. Our top tips to avoid getting caught out include:"

1. **Log into PayPal:** If you receive a suspicious email, don't act on the message or click on any links. Instead, open your browser, log into PayPal and check for any new activity. PayPal will also email or notify you in the app if you've received any payments.
2. **Check the basics:** Look out for misspellings and grammatical errors, which can be a tell-tale sign of a scam.
3. **Verify an email's authenticity:** Phishing scams will often mimic the look and feel of PayPal emails, and ask you for sensitive information – something that real PayPal emails will never do.
4. **How to spot the difference:** A PayPal email will address you by your first and last name, or your business name, and we will never ask you for your full password, bank account, or credit card details in a message.
5. **Avoid following links:** If you receive an email you think is suspicious, do not click on any links or download any attachments. You can check where a link is going before you click on it by hovering over it – does it look legitimate?
6. **Keep tabs on your information:** Limit the number of places where you store your payment information online by using a secure digital wallet like PayPal. If you are making a purchase online, consider using a protected payment method such as PayPal, so if your purchase doesn't arrive or match the product description, PayPal can reimburse you.
7. **Easiest of all, use common sense:** If a deal seems too good to be true, it probably is! Stay clear of exceptional deals or anything that is significantly reduced in price from what you would expect to pay.

If you think that you've received a PayPal related phishing email, you can forward it to spoof@paypal.com, without changing the subject line. PayPal will let you know whether it is fraudulent.

PBX/Dial-Through Fraud Threat

The threat of fraudsters hacking into school telephone systems has been mentioned on a number of previous occasions.

Schools can be targeted at any time of the year but are particularly vulnerable to telecom fraud when phones are left unmonitored for extended periods.

Depending on the type of phone system used, there are a number of ways a hacker may gain access to it. Incorrectly configured firewalls, poor security settings, lack of software maintenance and the use of default/easy passwords may all assist hackers to gain quick access.

Once access has been gained by criminals they can exploit in-built services such as voicemail, call forwarding and call diversion to direct calls to a number of their choosing. They tend to make financial gain by either dialling premium rate numbers that are associated with international calling companies, or by dialling international numbers through the compromised telephone system, most noticeably to Eastern Europe, Cuba and Africa. The fraud can result in schools being exposed to phone charges running into thousands of pounds.

The National Fraud Intelligence Bureau has issued details of some measures to reduce the risk of this fraud, namely:

- If you still have your voicemail on a default PIN/password change it immediately
- Use strong PIN/passwords for your voicemail system, ensuring they are changed regularly
- Disable access to your voicemail system from outside lines. This is usually used for remote workers to access. If this is not business critical then disable it, or ensure the access is restricted to essential users and they regularly update their PIN/passwords
- If you do not need to call international numbers/premium rate numbers, ask your telecoms provider to place a restriction on your telephone line
- Consider asking your network provider not to permit outbound calls at certain times (except 999), for example when your business is closed

- Ask your telecoms provider to alert you immediately if there is any unusual call activity taking place on your telephone lines
- Ensure you regularly review available call logging and call reporting options and regularly monitor for increased or suspect call traffic
- Secure your exchange and communications system, use a strong PBX (Private Branch Exchange) firewall and if you don't need the function, close it down
- If you use a maintenance provider speak to them, or ensure that the person responsible for the PBX understands the threats and ask them to correct any identified security defects
- Consider consulting your telecoms provider to ensure your settings for your PBX systems are secure and the settings have been properly set up.

If you have any questions, or would like further advice on any fraud related matters, please do not hesitate to contact Martin Curtis, Cornwall Council Counter-Fraud Senior Investigator, by emailing martin.curtis@cornwall.gov.uk