FraudSMART.

Informed. Alert. Secure.

Fraud Trends 2019

Niamh Davenport
Head of Fraud Prevention
6th March 2019

Banking & Payments Federation Ireland

Phishing - Email Fraud

Invoice Fraud

- Home buyer receives an email from fraudster pretending to be the estate agent.
- Seek deposit transfer and provide bank account details
- Buyer keen to secure property and transfers funds
- By the time the realisation that it was a fake email its too late and their funds have been transferred

Invoice Fraud Advice

- Never email or ask customers for bank details / transfers deposits over email. Either you or your customer's communications channel may have been compromised.

- Advise customers that it is not company policy to send bank account details via email. Often your clients may not be aware of this and if they receive an email will act on it.

- Make sure all security settings and software protection in your company, and on your computer, are up to date.

CEO Fraud

How CEO Fraud Can Impact Your Business

The Start

The fraudster spoofs your domain

Fraudsters often troll companies for months to gather the data necessary in pulling off a successful attack

The Phish

Spoofed emails are sent to high-risk employees in the organisation

To: Finance Dept.

Urgent transfer request. Please send €100,000 to new acct.

IE41 RANW 940109 20182012

To: CFO

Please pay this time-sensitive invoice. I'm on holidays and will be unavailable, no need to respond. - Your CEO

To: HR Dept.

I need a PDF copy of ALL employee P30s for Revenue ASAP!

The Response

Target receives email and acts without reflection or questioning the source

I better get this payment to the new account!

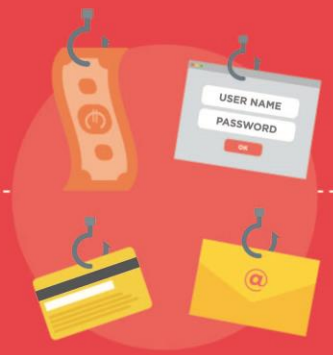
It's from the CEO, I'll take care of this for her!

Sounds important. I'll send these right away!

The Damage

Social engineering was successful, giving hackers access to what they were after

This leads to fraudulent wire transfers



The Result

The fallout after a successful attack can be highly damaging for both the company and its employees

Resulting damage:

- Money is gone and often not recovered
- Data Protection breaches may result
- Legal action
- Intangibles - tarnished reputation, loss of trust, etc.

So... Think Before You Click

CEO Fraud

Be Informed

- Always check with the person you believe sent the email that it is from them, no matter how senior or busy!
- Do not do this by email in case their account has been hacked. Instead, make a phone call, ask in person or use some other trusted communication method.

Be Secure

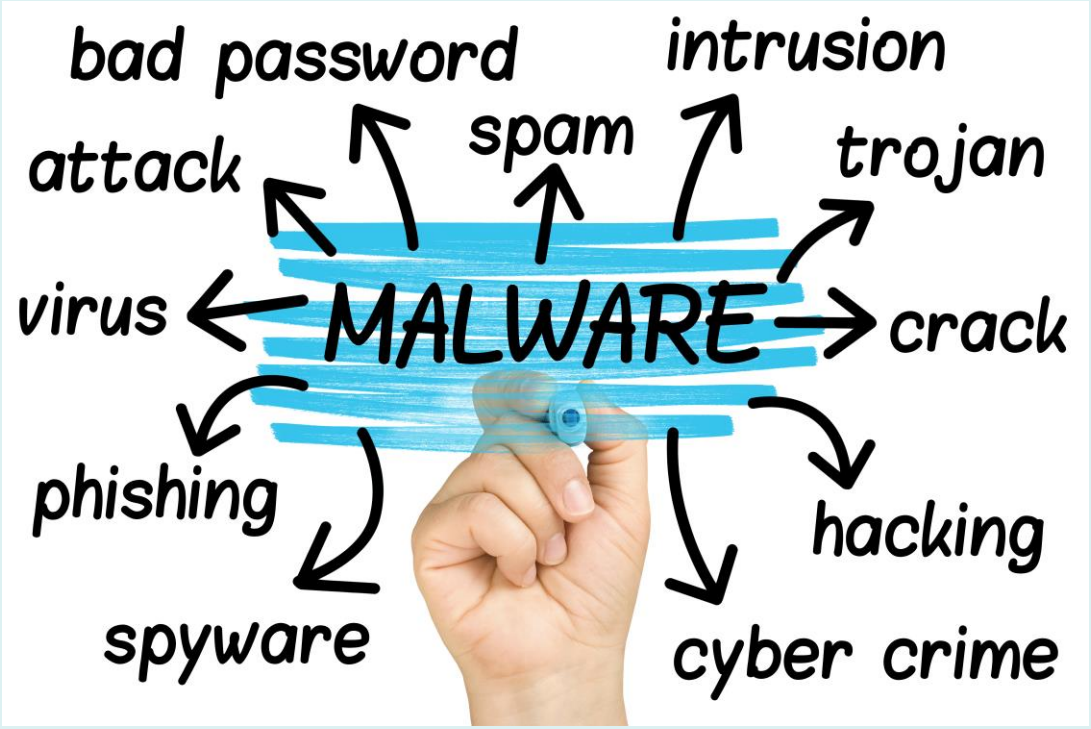
- Don't allow yourself to be rushed. Take your time and do the relevant checks.
- If in any doubt, do not make the payment, however urgent it may seem or whatever the suggested outcome(s).

Be Alert

- Be wary of payment requests that are unexpected or irregular, whatever the amount involved.
- Verbally verify bank account change requests from suppliers. Don't fall foul of the fraudster's tactic to send the email when the "sender" is away from the office making it difficult to verify with them. Do not email them.

Malware

- Malware is short for ‘malicious software’
- Designed specifically to disrupt and/or cause damage to your computer system.
- Banking Malware is a type of software used by cyber criminals to target online bank accounts and allows them to obtain personal and financial details.

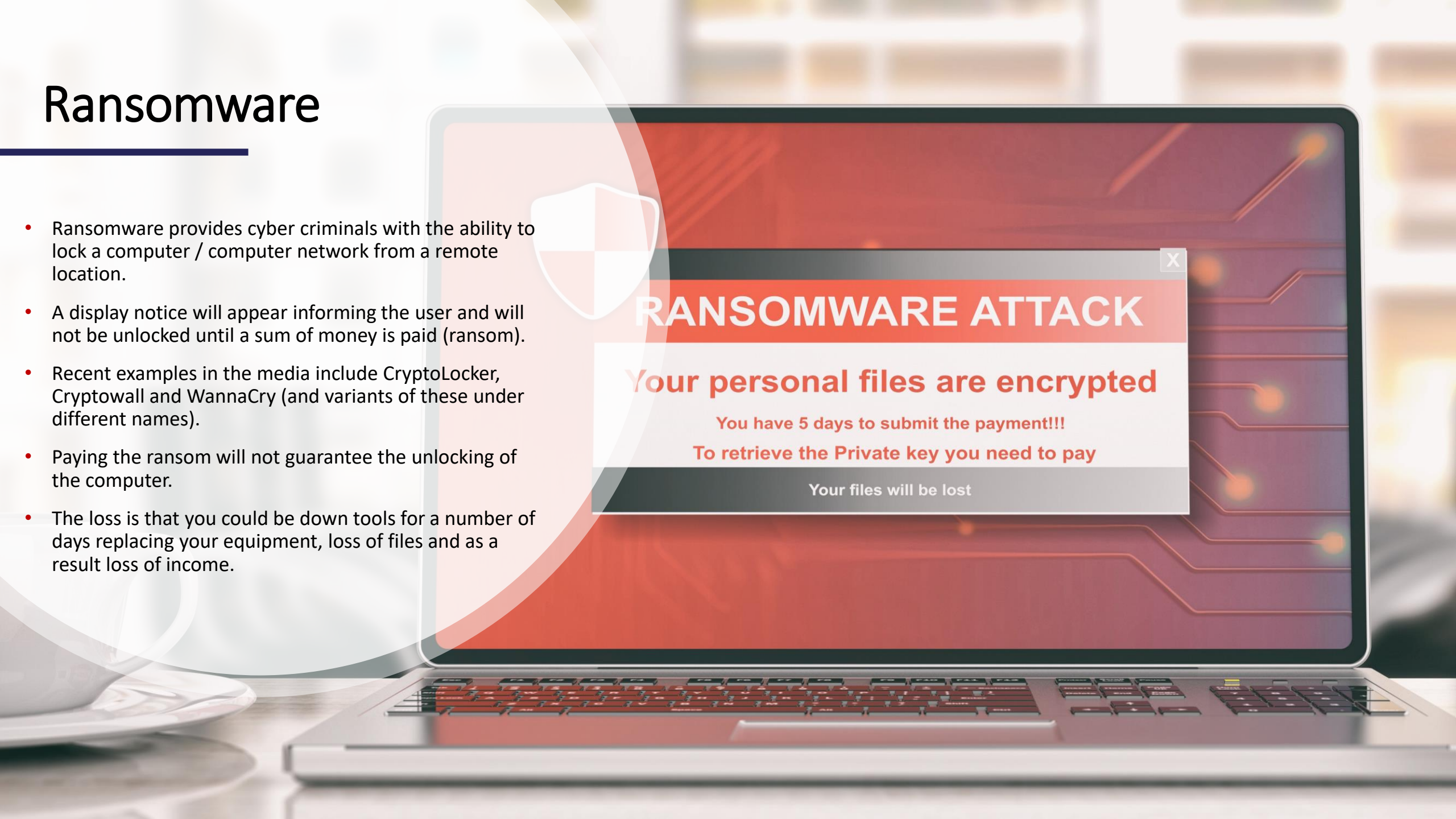


The signs to look for include:

- Advertising pop-ups (a window that opens on the screen) that appear every few seconds.
- Extra toolbars in your browser that won’t go away.
- Browser going to sites you didn’t tell it to.
- Unexplained system slowdowns.
- Sudden increase in computer crashes.

Ransomware

- Ransomware provides cyber criminals with the ability to lock a computer / computer network from a remote location.
- A display notice will appear informing the user and will not be unlocked until a sum of money is paid (ransom).
- Recent examples in the media include CryptoLocker, Cryptowall and WannaCry (and variants of these under different names).
- Paying the ransom will not guarantee the unlocking of the computer.
- The loss is that you could be down tools for a number of days replacing your equipment, loss of files and as a result loss of income.



Ransomware

Be Informed

- Never click on links in unsolicited emails, contact the sender to confirm the legitimacy.
- Always download mobile apps from official app stores.
- Regularly back up the data stored on your computer.

Be Alert

- Don't click or reply to attachments, banners or links without knowing their true origin.
- To detect and remove ransomware and other malicious software that may be installed on computers, run a full system scan with an appropriate, up-to-date, security solution.

Be Secure

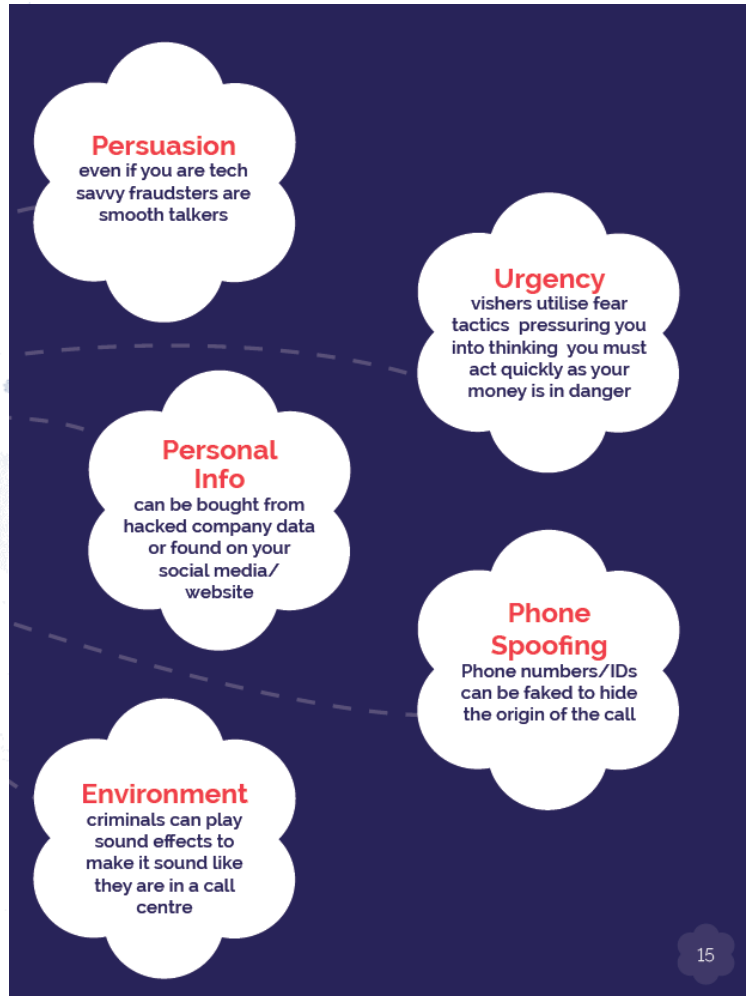
- Apply security patches as soon as possible after they become available from your technology providers.
- Update your software regularly with the latest security releases using only official and reliable software.
- Ensure you have a firewall enabled to protect your technology from the internet.

What to do when you have been attacked

- Seek professional advice from your security service provider or if you don't have one ensure you use a trustworthy source.
- Disconnect infected computers from your business network immediately to stop the spread of infection to other computers in your network.
- Advice from law enforcement agencies is not to pay the ransom. Paying does not guarantee that your problem will be solved and that you will be able to gain access to your files again.
- Report the attack immediately to the Gardaí. The more information that you give to the authorities, the more effective they can be in disrupting the criminal infrastructure behind these scams.

Vishing - Phone Fraud

Phone Scams - Techniques



54% of people said paying heed to their instincts would have prevented fraud

Phone Scams - Advice

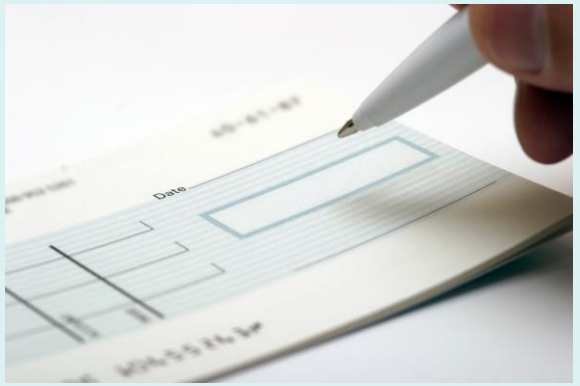
- Be very wary of unsolicited phone calls.
- Never divulge company or personal information until you have validated that the caller is a genuine representative of the organisation they claim to represent.
- Take the callers' number and advise them that you will call them back once you have validated their identity.
- Look up the organisation's phone number and make contact directly with them to validate.
- Remember that it takes two people to terminate a landline phone call, you can use a different phone line to independently check the callers identity.
- Never allow maintenance staff access to your payment terminals or tills unless you have independently verified their identity.

Cheque Scams

Cheque Scams

- **Counterfeit cheque fraud:**
  - Counterfeit cheques are manufactured or printed on non-bank paper to look exactly like genuine cheques and are drawn by a fraudster on genuine accounts held by the bank.
- **Fraudulently altered cheques:**
  - A fraudulently altered cheque is a genuine cheque that has been made out by the payer, but a fraudster has altered the cheque in some way before it was paid in, e.g. by altering the beneficiary's/payee name or the amount of the cheque.
- **Forged cheque fraud:**
  - A forged cheque is a genuine cheque that has been stolen from an innocent customer and used by the fraudster with a forged signature.
- **Funds not available:**
  - This is a genuine cheque; however there are no funds in the account to honour it.

- **Overpayment Scam:**
  - **A cheque is received for payment of service or goods.**
  - **The person making the payment by cheque writes for an amount larger than they owe.**
  - **They request the overpayment back by transfer.**
  - **Normally the company that received the overpayment does this before the cheque clears.**
  - **Cheque subsequently bounces and your company is down funds.**

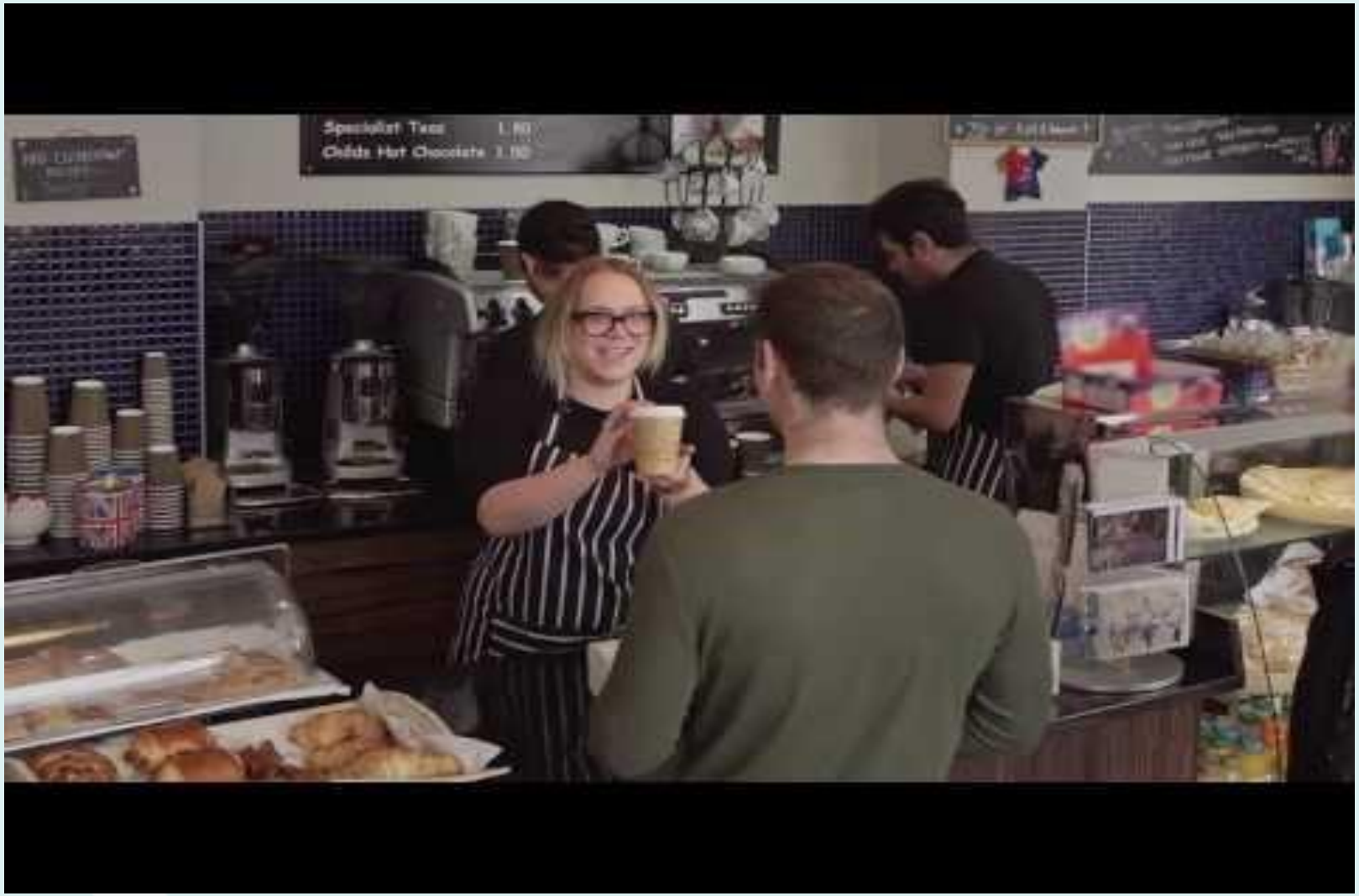


Cheque Scams- advice

- **Be Informed:**
  - Never issue a refund of a payment, either partial or full, until you are sure the cheque has cleared full and is not at risk of being rejected.
  - Cross all cheques a/c payee only
- **Be Alert:**
  - Ensure all issued cheques and unused cheques are accounted for.
  - Always exercise caution when forming new relationships with potential customers, undertaking appropriate due diligence.
- **Be Secure:**
  - Keep cheques in a secure place and control who has access.
  - Do not sign cheques in advance.
  - Never feel pressured into making a refund until you are sure the original funds are legitimate and secure.

Social Media

Data to Go!!!



https://youtu.be/_YRs28yBYuI

Thank You