Fraud SMART

Protect Your **Business** from Fraud

www.FraudSMART.ie

Banking & Payments Federation Ireland

AIB

Bank of Ireland

KBC

permanent tsb

Ulster Bank

Contents

FraudSMART

Most businesses would like to think that they are protected against fraud however fraud against Irish businesses is on the rise. While the majority of financial frauds still use telephone and emails to commit the crime, the frauds themselves are increasingly sophisticated. You are likely to get an email or a phone call from somebody you "know" and "trust". Fraudsters will manipulate their targets using what is known as 'social engineering' - essentially they use information that is publicly available to trick you into taking an action that may not be in your company's best interest.

With many advances in technical security to prevent banks and companies being hacked, fraudsters have turned to targeting businesses and consumers directly.

FraudSMART is a fraud prevention initiative which aims to raise consumer and business awareness of the latest financial fraud activity and provide simple advice on how best they can protect themselves and their money. Businesses can log onto FraudSMART.ie for a wide range of information and advice on the latest frauds and how to avoid being scammed.

Led by Banking & Payments Federation Ireland, FraudSMART is a joint initiative developed by the banking sector. Sign up on www.FraudSMART.ie for alerts on current fraud trends that may impact your business.

www.FraudSMART.ie
@FraudSMART
@FraudSMART

Top Tips to prevent fraud in your business

Be Informed

- Ensure employees are fraud aware and understand the controls and procedures in place to prevent fraud.
- Don't assume you can trust caller ID. Phone numbers can be spoofed so it looks like a particular company is calling even if it is not the real company.
- Fraudsters may already have basic information about you or your business in their possession (e.g. name, address, account details), do not assume a caller is genuine because they have these details.

Be Alert

- Be wary of payment requests that are unexpected, irregular or require changes to bank account details, whatever the amount involved.
- Always exercise caution when forming new relationships with potential customers, undertake appropriate due diligence.
- Always check your statements, and if you notice any unusual transactions, report them to your bank immediately.

Be Secure

- Don't allow yourself to be rushed. Take your time to do the relevant checks.
- If a supplier/service provider requests bank account details to be changed have a verification process in place before making payments.
- Ensure security and software is regularly updated and maintained using official and reliable software.

Email Scams

Invoice Fraud

Fraudsters pretend to be a supplier or service provider in order to trick you into changing bank account payee details on your online banking. An employee receives an email informing them of the new bank account details. Often there is no request for payment but all future payments will go this account controlled by the fraudster.

Your business orders from a supplier

Fraudster uses malware to access the details

Fraudster sends a fake invoice with new bank account details that looks legitimate

Your business pays money to the "new bank account" i.e. the fraudster's account

Be Informed

- Have a verification process in place before changing saved bank account details of your suppliers or service providers.
- Verify the change by contacting a known contact in the company directly, use contact details held on record or contact number on the company's website. Do not to use the contact details on the letter/email requesting the change as these could be fraudulent.
- Inform employees of this fraud so they are alert to it and can avoid it.

Be Alert

- Fraudsters can change an email address to make it look like it has come from someone you email regularly. Look out for different contact numbers and/or a slight change in the email address e.g. .com instead of .ie as these may differ from previous correspondence.
- The first contact may inform you of a change in bank account details but not request payment. This ensures that all future payments are sent to the new account.

Be Secure

- Fraudsters may have found information regarding contracts and suppliers on your company's own website. You should consider if this information really needs be on your website for fraudsters to utilise.

CEO/Executive Impersonation Fraud

The fraudster impersonates the CEO or a Senior Executive from your company. A legitimate email account is hacked to get an employee to unwittingly transfer funds.

For example, the fraudster will hack into the CEO's email account and send an email to an employee requesting them to make a payment to a supplier. Bank account details may be provided in the email or an existing supplier who has recently sent a change request to the finance team. This results in the funds ending up in the fraudsters account and not your suppliers.

65%

of people said they could have prevented fraud by checking the legitimacy of unexpected emails/texts before clicking on links within them

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 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.

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).

How CEO Fraud Can

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!

Impact Your Business

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

Phone Scams

Vishing (Voice and Phishing) is a phone scam where fraudsters target a business by phoning and claiming to be your bank, card issuer or service provider e.g. computer support looking to talk you through a procedure over the phone to "upgrade your system" or somebody claiming to represent your payment terminal maintenance.

Fraudsters try to extract details such as information about your computer system, business details, debit or credit card details, PIN number, online banking details and passwords. This can then be used to gain access to company bank accounts, carry out transactions or steal personal customer information.

54%

of people said paying heed to their instincts would have prevented fraud – if something doesn't feel right it generally isn't...

Be Informed

- Never divulge personal or business information until you have validated that the caller is a genuine representative of the organisation they claim to represent. Hang-up, look up the number independently and call back, make sure you hear a dial tone before you dial.
- Don't assume you can trust caller ID. Fraudsters can spoof their numbers so it looks like they are calling from a particular company, even when they're not.
- Your bank or the Gardaí/Police will never ask you for your credit or debit card PIN number or full online banking password.
- Your bank will never request you withdraw money to hand over to them or transfer money to another account, even if they say it is for safekeeping.

Be Alert

- Remember that it takes two people to terminate a landline phone call; you can use a different phone line to independently check the caller's identity.
- Fraudsters may already have basic information about you or your business in their possession (e.g. name, address, account details), do not assume a caller is genuine because they have these details.

Be Secure

- Take the caller's number and advise them that you will call them back once you have validated their identity.
- Use a phone number from the phone book or their website, not one given to you by the caller (this could be fake). If the caller is genuine, they will understand and welcome your need to validate them.
- Don't allow yourself to be rushed. Take your time and do the relevant checks.

Vishing techniques to be particularly aware of

Persuasion

even if you are tech savvy fraudsters are smooth talkers

Urgency

vishers utilise fear tactics pressuring you into thinking you must act quickly as your money is in danger

Personal Info

can be bought from hacked company data or found on your social media/ website

Phone Spoofing

Phone numbers/IDs can be faked to hide the origin of the call

Environment

criminals can play sound effects to make it sound like they are in a call centre

Malware

Malware is 'malicious software' designed to damage or do other unwanted actions on a computer system. Common examples include viruses, worms, Trojans, and spyware.

Cyber criminals use malware to target online bank accounts and obtain personal and financial details. It runs undetected in the background, often hidden in free software that you download from the internet or a multimedia program/file such as music or a video

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.

52%

of people said they could have prevented fraud by not opening email attachments until they independently verified the email was from the company that sent it

Ransomware

Ransomware locks users out of their devices or blocks access to files until a sum of money or ransom is paid.

Attacks cause downtime, data loss, possible intellectual property theft, and a possible data breach. You could be down tools for a number of days replacing your equipment and loss of files and as a result suffer a loss of income.

Most commonly users receive an email, claiming to be from a legitimate company, containing malicious content. The ransomware runs when attachments or links in the email are clicked. It encrypts every file on the user's device and on any fileshare to which they are connected. A blocking screen appears ordering the user to pay a ransom in order to regain access to their files. If the user does not pay the ransom on time, all files may be lost.

One function generally available to the user is a number keypad to enable payment, often requested in the form of Bitcoin. Paying the ransom will not guarantee the unlocking of the computer.

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.

Cheque Fraud

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 it for an amount larger than they owe (i.e. they make an overpayment). They then request for the business to send the overpayment back by cheque or refund to an account. This is done before the cheque clears, which is usually returned unpaid or is written from a bogus account, leaving the business with a loss of funds.

Be Informed

- Never issue a refund of a payment, either partial or full, until you are sure the cheque has cleared fully and is not at risk of being rejected (usually cleared on sixth working day).
- When sending cheques in the post, send securely and avoid using window envelopes.
- Cross all cheques 'a/c payee only'.

Be Alert

- Ensure all issued cheques and unused cheque numbers are accounted for. Check this when you get a new cheque book and review regularly to ensure no cheques are missing.
- Always exercise caution when forming new relationships with potential customers, undertaking appropriate due diligence.

Be Secure

- Keep cheques in a secure place.
- Control who has access to cheque books.
- Do not sign cheques in advance.
- Never feel pressured into making a refund until you are sure the original funds are legitimate and secure.

Card Fraud

Shopping online has grown significantly and from a business perspective it offers access to new customers and markets. Accepting cards remotely can pose retailers with a challenge, with neither the card nor the cardholder present when the transaction takes place – how do you know the transaction is genuine?

There are a number of tools and techniques that can be utilised by retailers when selling remotely including building up a profile of the customer and authenticating the cardholder to ensure they receive payment securely.

Be Informed

- Ensure that you have the correct terms in place with your card processor. You must revise your terms with your card processor if you are moving from solely a face to face business to accepting payment cards over the internet.
- You can be held financially accountable for an unsecured fraudulent transaction, even if the card issuer has provided an authorisation code during the sale. The authorisation from the card issuer confirms the funds are available to cover the sale amount and that the card was not reported lost or stolen at the time of the transaction. It is the retailer's responsibility to ensure that the genuine cardholder is carrying out the sale.
- Ensure all staff including those on temporary or part-time cover are familiar with what to watch out for.

Be Alert

- Be particularly careful if the goods purchased are of a high value and easily re-saleable as this makes them a more likely target for fraudsters.
- Be wary of unusually large or high value orders or orders that are being delivered to countries you would not normally do business with.
- Check records of previous orders for anomalies or suspicious trends. Watch out for the same card number being used with different delivery addresses, the same delivery address/contact number being used with different card numbers or orders that don't make sense e.g. much larger or more frequent orders than you would typically expect.
- Always check the credentials of new customers, particularly if placing a high value first order or making multiple orders in a short timeframe.
- Be cautious of rush orders, collections or last minute changes in delivery address. Criminals often create a time pressure so that you do not have time to carry out normal checks.

Be Secure

- Use 3D Secure as it gives more protection against fraud related chargebacks.
- Check the delivery address is valid. Avoid deliveries to PO boxes.
- If a purchaser calls to collect the goods in person, ask to see the card that was used in the purchase. Collections by taxi, courier or other third parties are not recommended.

Safe Online Banking

Internet banking is a very convenient and efficient way to conduct your business banking needs however it is vital to protect your passwords and secure log in details to prevent fraudsters gaining access to your accounts.

You or your colleagues could be tricked by phishing emails or vishing telephone calls into disclosing your password and details on fake banking websites, or to bogus callers. Fraudsters can gain access to funds either by getting you to transfer money to an account or asking you for details to allow them to make transactions themselves. They can also install malware on your system giving them access to your bank accounts and other security information stored on your computer which they can then use for identity theft.

Be Informed

- Never disclose your security details, PIN, full online banking or personal information in response to an email, phone call or letter claiming to be from your bank or other financial institution. Your bank would never ask you to disclose these.
- Your bank will never send you an email with a link to a page that asks you to enter your online banking details.
- Only ever visit your bank's website by entering the address into your browser or using a bookmark you have created using the correct address.

Be Alert

- Be aware of 'shoulder surfers' viewing your screen.
- Always check your statements, and if you notice any unusual transactions, report them immediately.
- Treat any unexpected requests to change payee or supplier's bank account details with caution. Double check the details.
- Always log out of internet banking sessions once you have finished.

Be Secure

- Never use public Wi-Fi for online banking. Use a 3G/4G connection.
- Look for 'https' at the beginning of the address and the padlock symbol in the browser frame.
- Ensure you have effective and updated antivirus/antispyware software and firewall running before you log in to your bank account.

What to do if you are a victim of fraud?

If you suspect you have been the victim of fraud or have noticed unusual activity on your bank account(s) contact your bank immediately and also report to your local Garda Station. Fraudsters move fast; the quicker you contact your bank to safeguard your accounts the better.

AIB	**Internet Banking Transactions:** From Outside ROI **AIB Debit/Credit Card Transactions:** **iBusiness Banking Transactions:** From Outside ROI Opening Hours: Mon-Fri 08.30 – 17.30	0818 724 724 +353 1 771 2424 01 668 5500 0818 720 000 +353 1 641 4889
Bank of Ireland	**365 Online:** From Outside ROI Forward suspicious emails to: **Lost/Stolen Cards 24 Hr** From Outside ROI: **Business On Line:** Opening hours: Mon-Fri 08.00-18.00 Closed Saturday, Sunday, Bank Holidays	0818 365 365 +353 1 4044000 365security@boi.com 1890 706 706 +353 56 775 7007 1890 818 265
Permanent tsb	Card related issues From Outside ROI Alternatively the Fraud Dept. All other fraud queries Your local branch is also available to deal with any suspected fraud queries	1890 500 121 +353 1 2124101 +353 1 6695851 1890 500 121
Ulster Bank	Fraud Notifications	1800 245 403
KBC Bank Ireland	**Customer Support Team** **Card Fraud – Card Security Team**	1800 93 92 44 1800 93 62 87 alert@kbc.ie

You should also report suspected fraud incidents to
An Garda Siochana via your local Garda Station.
https://www.garda.ie/en/Contact-Us/Station-Directory/

FraudSMART.

Informed. Alert. Secure.

FraudSMART was created by

Banking & Payments Federation Ireland

Banking & Payments Federation Ireland,
Nassau House, Nassau Street,
Dublin 2, D02Y240, Ireland

Phone +353 1 671 53 11
Email info@fraudsmart.ie