



**CYBER
SAFETY**

Cyber Threat Awareness & Responses:

A Practical Guide for Crime Victims

Cyber Safety for Vulnerable Populations,
2025.





CYBER
SAFETY

Table of Contents

Table of Contents	1
Introduction	2
If Your Information Has Been Compromised	3
Phishing	4
Online Sales Fraud	6
Romance Scams	7
Sextortion	8
Ransomware	9
Lottery Scams	11
Rental Scams	12
Law Reform	13

Introduction

About This Document

This is a reference guide or “cheat sheet” on common cyber safety pitfalls and tips, which was developed by researchers at Munster Technological University. It is designed to give you a way to study or quickly check the types of scams that are out there, how to recognise them, and what recourse may be available if you or someone you know has fallen victim to these scams. The cyber threat landscape is constantly developing and we are open to user feedback on the document; please visit our website to contact us with feedback at cybersafety.ie.

The Team Behind It

The Cyber Safety Team at Munster Technological University developed this resource. We are an interdisciplinary group of researchers specialising in cyber advice, user experience, learning development, psychology, vulnerable groups, cyber security, and universal design. We are recently multiply published on cyber safety topics. You can follow our team on LinkedIn [here](#) (or search Cyber Safety MTU) and see our free resources for learning cyber safety on our [website](#).

Advice Disclaimer

The information provided in this document is for information purposes only and does not constitute legal advice. While every effort has been made to ensure the accuracy of the information, it is not intended to replace professional legal consultation. For specific legal advice, please consult a practising solicitor.

Our Funding

This project was conducted with the financial support of the EU Commission Recovery and Resilience Facility under Research Ireland Our Tech Grant Number 22/NCF/OT/11212G.

If Your Information Has Been Compromised

Before we delve into more detailed advice about types of cybercrimes and online safety, it's important to know what actions to take if you believe one of your accounts has been hacked or accessed without your permission.

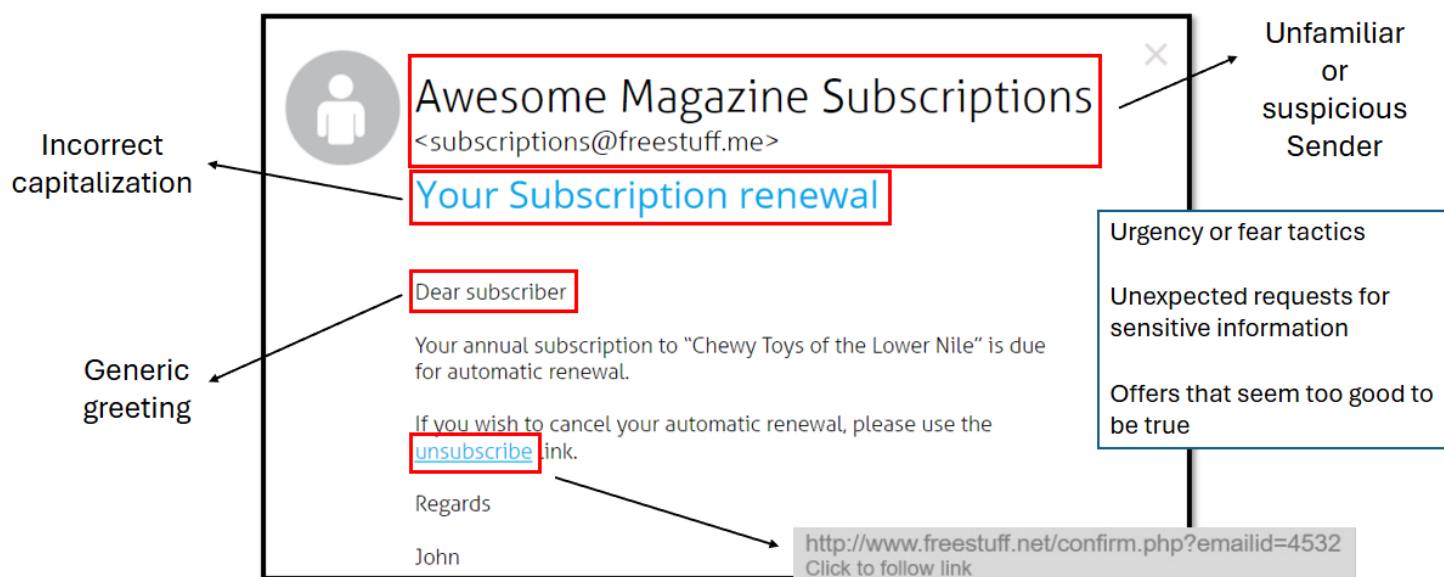
Here are the immediate steps you can take to help protect yourself and limit any harm.

1. First, immediately change any passwords you believe are compromised. If there is a **“Log out of all devices”** option, select this to remove any unauthorised access to your accounts.
2. Then, you should contact the compromised account’s service provider through their official channels *(For example, your bank, through the helpline listed on your physical bank card or An Post, through their website)*.
3. Following this, check your other important accounts that contain sensitive personal information or payment details for any further unusual activity. Then, check your other accounts, such as your email, banking, or any other account that contains personal or banking details. This can avoid multiple accounts being compromised, or malicious messages being sent to your contacts.
4. You can contact your local Garda station to report the crime and request a **PULSE ID**. This is a number allocated to an incident in the Garda system, which means the Gardaí have opened a criminal case.
5. You can then provide the PULSE ID to your service provider to show that you were a victim of a crime, and to keep track of the ongoing investigation.

Phishing

What Is It? A type of cyberattack where scammers impersonate trustworthy entities to trick individuals into sharing sensitive information such as passwords, credit card details, and PIN's.

How to Recognise It?



What is the Law? Cardholder/Accountholder obligations: 1. Keep personalised security credentials safe i.e. passwords, credit card details, PIN number (Article 69.2, [Payment Services Directive 2015](#)) 2. Notify the bank/card issuer as soon as the cardholder becomes aware the loss, theft, misappropriation or unauthorised use of the card/account ([Article 69.1.b. Payment Services Directive](#))

What Can You Do? Report all phishing attacks to local Gardai ([how-to here](#)). Report card/account compromise to card issuer/bank to limit liability. Understand that recovery of funds is a limited possibility, depending on how the payment was made. For credit card-enabled fraud, a chargeback procedure may be an option through the provider. For direct debits, you have the right to request a refund.

Phishing *(continued)*

Limiting Liability: *You can limit liability for a lost, stolen, or misappropriated credit card. Notify the card issuer that the card or account has been compromised. For any subsequent unauthorised payments, the maximum liability is €50. There is no protection if the card holder has committed fraud or been ‘grossly negligent.’ There is no definition of ‘gross negligence’ in the Directive, except a ‘significant degree of carelessness’ per a case-by-case assessment. Example: keeping the PIN or other credentials used to authorise a payment transaction for bank app/website in a format that is open and easily detectable by third parties. Source: [Payment Services Directive Article 74.1](#)*

More on Credit Card Refunds: *A chargeback procedure is not a legal right, but a contractual one that is subject to conditions. The reason must be that the transaction was fraudulent and not authorised by the cardholder. With Visa and Mastercard it must be within 120 days of the original transaction. If taking this route provide all details like emails or account details. There is no guarantee of success.*

More on Direct Debit: *Account holders have some rights under the [Payment Services Directive](#). This applies to payments made by direct debit only. You can request repayment within 8 weeks of the payment date without giving a reason as per Article 77.1. You request repayment within 13 months of the payment date for an unauthorised payment – BUT must act ‘without undue delay’ once you become aware of the unauthorised payment as per Article 71.1.*

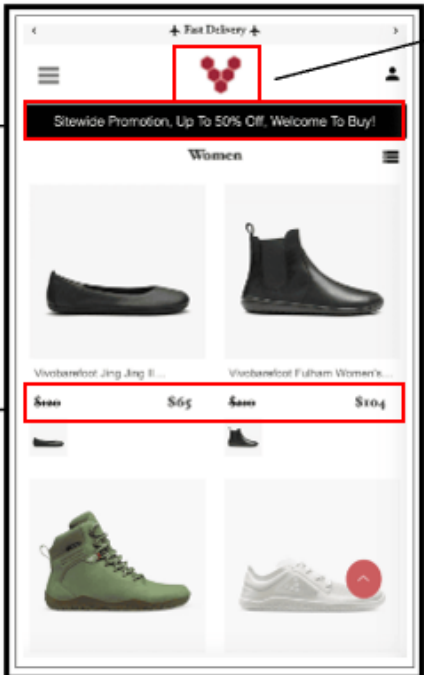
If You Were Phished through a PayPal QR Code: *As part of a very limited compromise on the part of PayPal, if you buy something from a seller in-person by using a PayPal goods and services QR code, your transaction may be eligible for PayPal Buyer Protection. This is limited to within 180 days of the original payment. Find more details at [PayPal's Buyer Protection Program](#).*

Online Sales Fraud

What Is It? *Deceptive practices used in online marketplaces or e-commerce platforms to scam buyers or sellers out of money, goods, or personal information.*

Common Examples: *Fake online stores, classified scams, concert ticket scams, rental scams, holiday rental scams*

How to Recognise It?



The screenshot shows a mobile app interface for a shoe store. Several red boxes highlight suspicious elements:

- Pixelated images:** A red box around the store's logo in the top navigation bar.
- Bad grammar:** A red box around the promotional banner text: "Sitewide Promotion, Up To 50% Off, Welcome To Buy!".
- Bargain-basement prices:** A red box around the product prices: \$200, \$65, \$200, and \$104.

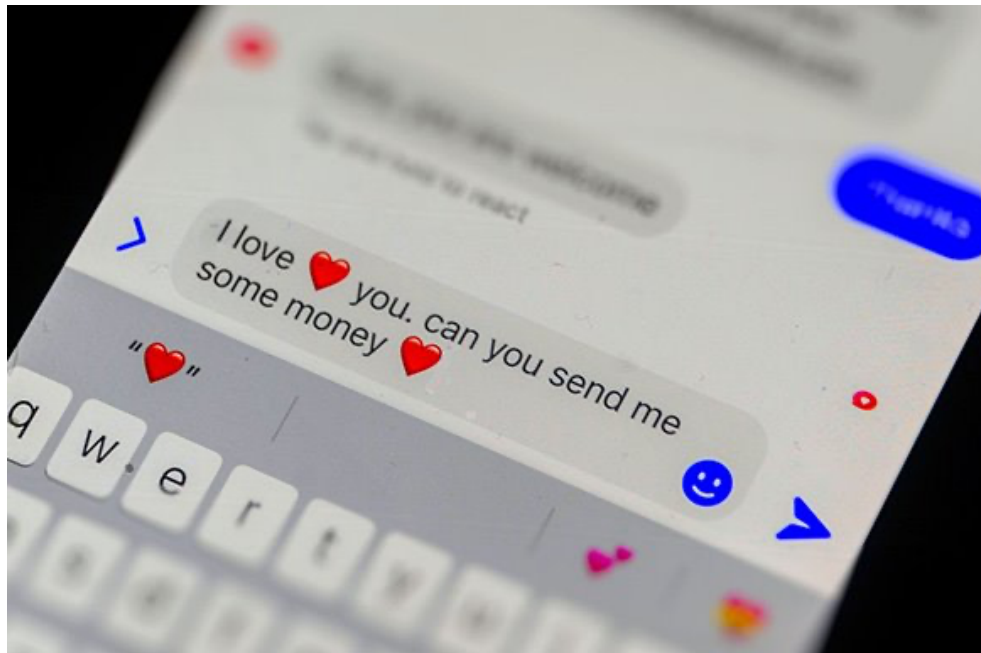
Other red flags listed in a box on the right include:

- Limited contact details
- Complex or non-existent returns policy
- Questionable payment options
- Check social media presence and customer reviews

What Can You Do? *Report all online sales fraud to local Gardai ([how-to here](#)). Call your bank to have your card cancelled and replaced. If using credit card, Revolut, or PayPal, request a chargeback procedure. For all other online sales frauds, refer to the Phishing section.*

Online Sales Fraud Chargeback Procedure: *Chargeback procedures are not a legal right, but a contractual right subject to terms and conditions. It is available where goods or services were not received. First contact the seller in writing and make a formal complaint. Then escalate to the payment services provider and use their procedures. For a credit card transaction, contact the bank. For PayPal check terms and conditions [here](#) and for Revolut check them [here](#). Provide evidence like emails, texts, and receipts.*

Romance Scams



What Is It? Scammers using fake identities to gain trust and affection online, exploiting the illusion of a relationship to manipulate or steal from victims.

How to Recognise It? Romance scammers push to move communication off dating sites to messaging, text, or calls. They may ask many personal questions but avoid sharing anything about themselves. Their stories may seem inconsistent (e.g., claim to be educated but have poor grammar) and their life circumstances may seem overly dramatic. They may quickly try to form a bond, often using pet names. They may ask for financial help, citing money problems. They may avoid meeting in person or on video calls, making excuses or cancelling plans last minute. Ultimately, they request money transfers or other payments from the victim.

What Can You Do? Report a romance scam to local Gardai ([how-to here](#)). If you shared credit/debit card/ID details, then alert your bank to cancel your card and get a replacement. If you willingly bought goods and services, a chargeback may be possible but is unlikely. If you sent money, it is unlikely to be recovered.

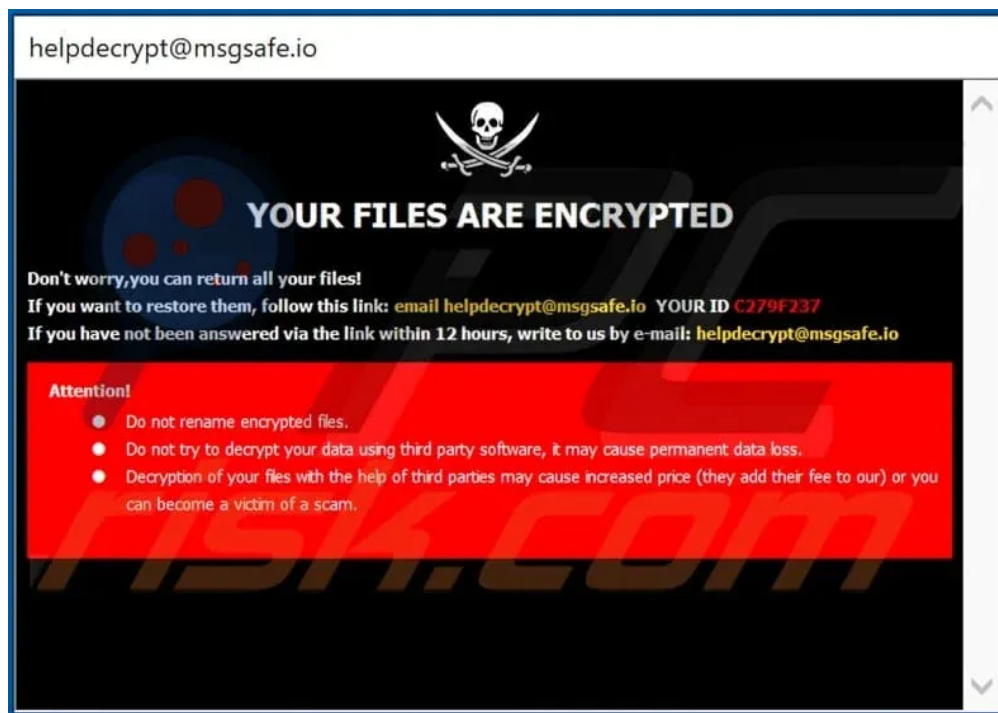
Sextortion

What Is It? A form of cyber extortion which involves a threat or blackmail of having intimate information, images or clips shared without consent. Sextortion can occur in several ways: Victims can be either partner in a relationship, whether it's ongoing or broken; intimate images might be shared online with strangers or known individuals; images might be posted via messenger apps. Juveniles sharing intimate images risk sextortion, bullying, and involvement in child sexual abuse material.

How to Recognise It? The relationship is moving very fast, expressing strong emotion and suggesting you get nude or sexual on a video call. Their profile does not match what you see or hear when talking with them. They ask for help, financially. They say their web cam is not working and may send nude photos which they claim to be them. They may say you have been hacked, or they have access to your contacts.

What Can You Do? Report Sextortion to the local Gardai - [Here's how and some FAQs](#). The [Harassment, Harmful Communications and Related Offences Act 2020](#) ('Coco's Law') states sextortion as a criminal offence. Report to social media platforms such as Facebook, Instagram, and X, and lodge complaints about content posted via the online abuse reporting links. If money was sent, contact your bank and cancel and replace your card. Keep all texts, emails, and messages for evidence in case of prosecution. Other options will depend on the facts of the case – consult a solicitor. If experiencing significant distress related to the violation, seek triaging for support services through [Rape Crisis Ireland](#).

Ransomware



What Is It? A type of malicious software that locks or encrypts a victim's files or systems, rendering them inaccessible. The attacker demands payment in exchange for restoring access. Some examples of types of ransomware attacks: Types of ransomware attacks: Crypto Ransomware (encrypts files); Locker Ransomware (locks you out of your device); Scareware (uses scary messages to trick you); Doxware (threatens to leak your private data); and Wiper Malware (which deletes data without financial gain).

How to Recognise It? Ransomware **delivery methods** could include phishing emails, compromised websites, or pirated software. Ransomware can be **executed** through encrypted files (e.g. [.akira](#) or a [string including HELLO or HELP+ numbers](#)) or a ransom note including the payment method, deadline, and a threat of data loss or publication. **Payment methods** are usually untraceable methods such as BitCoin.

What Can You Do? Don't pay the ransom. Check www.nomoreransom.org, a Europol service offering decryption codes that may unlock the device. If you already paid, contact your bank and request reversal of money transfer (unfortunately this has a low success rate). If you paid with BitCoin, this is not recoverable as it is not supervised by the Central Bank. You might also contact an IT specialist.

Investment Scams



What Is It? Scams that offer you high returns on money invested. These scams often prey on people's desire to grow their wealth quickly or with minimal risk. Common investment scams often involve enticing opportunities in areas such as stocks, bonds, cryptocurrencies, precious metals, foreign real estate, or alternative energy projects.

How to Recognise It? Investment scams may have a sense of urgency, indicating there is limited time to invest. They may use complex jargon, making the scammers seem like experts - yet no real information is being revealed. Scammers might make it seem like the opportunity is too good to miss, and the user would be a fool not to take it. The offer might include high reward for little risk. There may be an initial return on first investment to reel you into giving more before they disappear. Scammers might request or pressure for secrecy, telling you not to tell family and friends.

What Can You Do? Investment scams are a complex crime. Report to the local Gardai -- [Here's how and some FAQs](#). Notify your bank, cancel any credit or debit cards used, and change passwords and login details where applicable. If you initiated through direct debit, you may have some repayment options if under 8 weeks (see phishing section). If you paid through money transfer, you can contact your bank and request a reversal, though unfortunately this has a low success rate.

Lottery Scams



CONGRATULATIONS!!

Your Email was selected in Powerball Lottery
Draw with the sum of 1.5million dollars.
Kindly send your Full Name, Address and
Phone Number for claims.

Yours Sincerely
Mr. James Hodges
Head Of Operations

What Is It? In a lottery scam, scammers trick people into thinking they have won a large lottery or prize. The scam is designed to fool victims into providing personal information or sending money to the fraudsters to claim their "winnings."

How to Recognise It? A lottery scam attempt might comprise of: unexpected notifications or attempts at contact; request for payment, like a fee or payment details; or promises of more prizes: once victims pay a fee, they might receive more messages claiming that additional "taxes" or "fees" are due before they can claim their prize. Some other telltale signs of a lottery scam include: victims didn't enter any lottery or drawing; scammers request money (legitimate lotteries don't need fees); urgency or pressure around taking action; unpolished communication like grammar mistakes; suspicious email address or phone number; unrealistic or outlandish offers; or unverifiable information, like no web or media presence for the lottery provider.

What Can You Do? Notify your bank and cancel any credit or debit cards used. You may be eligible for a chargeback procedure if you used your credit card; however this is a contractual right in some contracts and not a legal right, so it will depend on the card provider. If you initiated through direct debit, you may have some repayment options if under 8 weeks (see phishing section), or it may be possible that the bank transfer hasn't cleared and your bank may catch it if you act quickly. If you paid through money transfer, you can contact your bank and request a reversal, though unfortunately this has a low success rate.

Rental Scams

What Is It? *A rental scam occurs when someone falsely advertises a rental property—whether it's a house, apartment, or vacation rental—to trick potential tenants or renters into paying money for a property that may not exist, is unavailable, or the scammer has no right to rent.*

How to Recognise It? *Rental prices might unusually low for the area or the property type, as scammers often offer unrealistic deals. Another red flag is when the landlord or "property owner" pressures you to make a decision quickly, often urging you to send money before you've had a chance to view the property in person or thoroughly inspect the lease terms. If the landlord is unwilling or unable to meet in person or show the property, that's another sign of a potential scam. Additionally, scammers may only communicate through email or text messages and avoid phone calls, which can make it harder to verify their legitimacy. If the listing has vague or poorly written descriptions, or if the photos seem overly polished or generic (often taken from other sources), it might indicate a scam. You may be asked to wire money or send payments through unconventional methods like gift cards or BitCoin, which are hard to trace and recover. To stay safe, make sure to research the property, verify the identity of the landlord, and inspect the rental before making any financial commitments.*

What Can You Do? *Report rental scams to local Gardai ([how-to here](#)). Report card/account compromise to card issuer/bank to limit liability. Understand that recovery of funds is a limited possibility, depending on how the payment was made. For credit card-enabled fraud, a chargeback procedure may be an option through the provider, but this is a contractual right for some credit card contracts, not a legal right. For direct debits, you have the right to request a refund under the [Payment Services Directive](#). This applies to payments made by direct debit only. You can request repayment within 8 weeks of the payment date without giving a reason as per Article 77.1. You request repayment within 13 months of the payment date for an unauthorised payment – BUT must act 'without undue delay' once you become aware of the unauthorised payment as per Article 71.1.*

Law Reform

United Kingdom: *as of the 7th of October 2024, the UK passed legislation taking measures to protect victims of purchase fraud, impersonation fraud, investment fraud, romance fraud, invoice fraud, and other types of “authorised push payment fraud” or payments authorised under fraudulent circumstances. For authorised push payment fraud committed on or after 7 October, 2024, there is now legal recourse in the UK. Reimbursement is capped at capped at £UK85,000 and for UK residents only. Read more [here](#).*

European Union: *There is a proposed amendment of the Payment Service Directive to give victims of fraud a right of refund by their bank or other PSP, in specific circumstances, as well as to implement tighter controls on payee identification. As of January 2024, this legislation is in its early stages.*



CYBER SAFETY