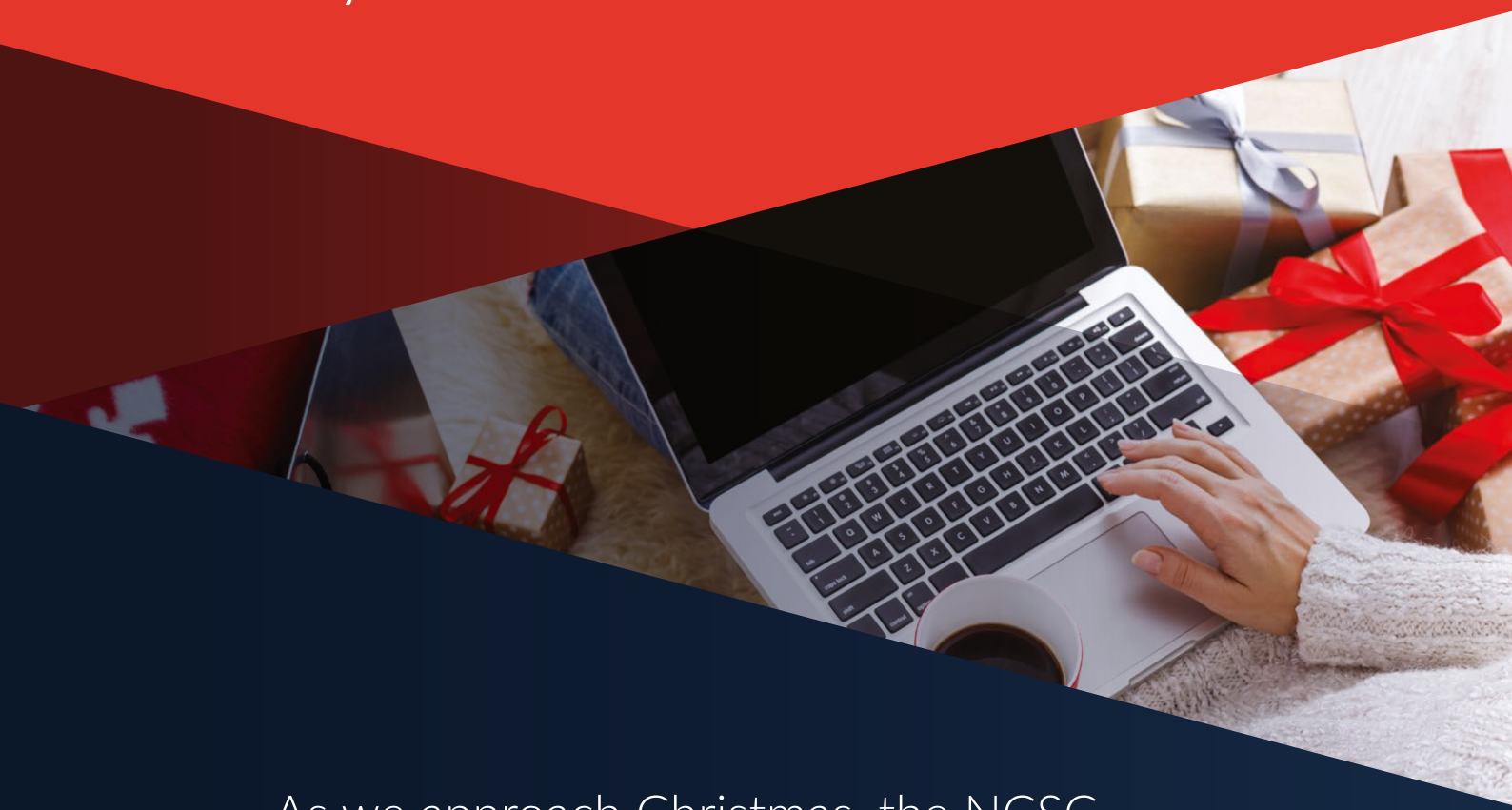
An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

NCSC
National Cyber
Security Centre

Seasonal
Cyber Awareness



As we approach Christmas, the NCSC would like to take this opportunity to remind people that this is a particularly active period for cyber criminals to take advantage of unsuspecting online shoppers.

www.ncsc.gov.ie

Introduction

As we approach Christmas, the NCSC would like to take this opportunity to remind people that this is a particularly active period for cyber criminals to take advantage of unsuspecting online shoppers.

In the weeks approaching Christmas and with events such as "*Black Friday*" and "*Cyber Monday*", there is a marked increase in online shopping which in turn creates more opportunities for malicious actors and online scams.

The Banking Payments Federation of Ireland (BPFI) have reported that fraudsters stole nearly €85 million (€84.6m) through frauds and scams in 2022, an increase of 8.8% on 2021[1]. The BPFI report also highlights the continued rise in the value of unauthorised electronic transfers (primarily payments through mobile and online banking) which accounted for almost 39% of fraud losses at €32.8m.

Phishing

Phishing emails are still the most common attack vector that we observe, in the second quarter of 2023, the Anti PhishingWorking Group (APWG), a not-for-profit industry association, observed 1,286,208 phishing attacks. This was the third-highest quarterly total that the APWG has ever recorded[2]. For this reason the NCSC would like to ensure that people are prepared to defend themselves from cyber related threats during this busy season.

Whilst email phishing is still the most common attack vector for such crimes, mobile phone users are also being targeted through text or SMS phishing (smishing) and through malicious links embedded in popular messaging & social media apps. There has been a noted increase in reports of fraudulent text messages.

[1] https://www.fraudsmart.ie/2023/07/14/fraud-losses-reached-almost-e85m-in-2022-as-consumers-warned-to-be-on-highalert-for-text-message-scam/

[2] https://docs.apwg.org/reports/apwg_trends_report_q2_2023.pdf

Common themes for these smishing attempts include:

Customs or Irish Revenue requesting that a **customs charge be paid for a package** or delivery

Fake refund or shipment tracking sites that attempt to harvest credentials including usernames/passwords/credit card details often impersonating An Post

Banks requesting confirmation of your online banking **information or passwords**

A family member that has lost their phone and needs money sent to them for an emergency **("Hi Mum..." scam)**

A official or legal authority alleging that **you have committed an offence and need to make a payment in order for criminal proceedings to be halted**. The success of these tactics are based on the use of social engineering techniques, to invoke a specific response, normally fear or panic, from victims and cause them to act urgently and without considering all the information available.

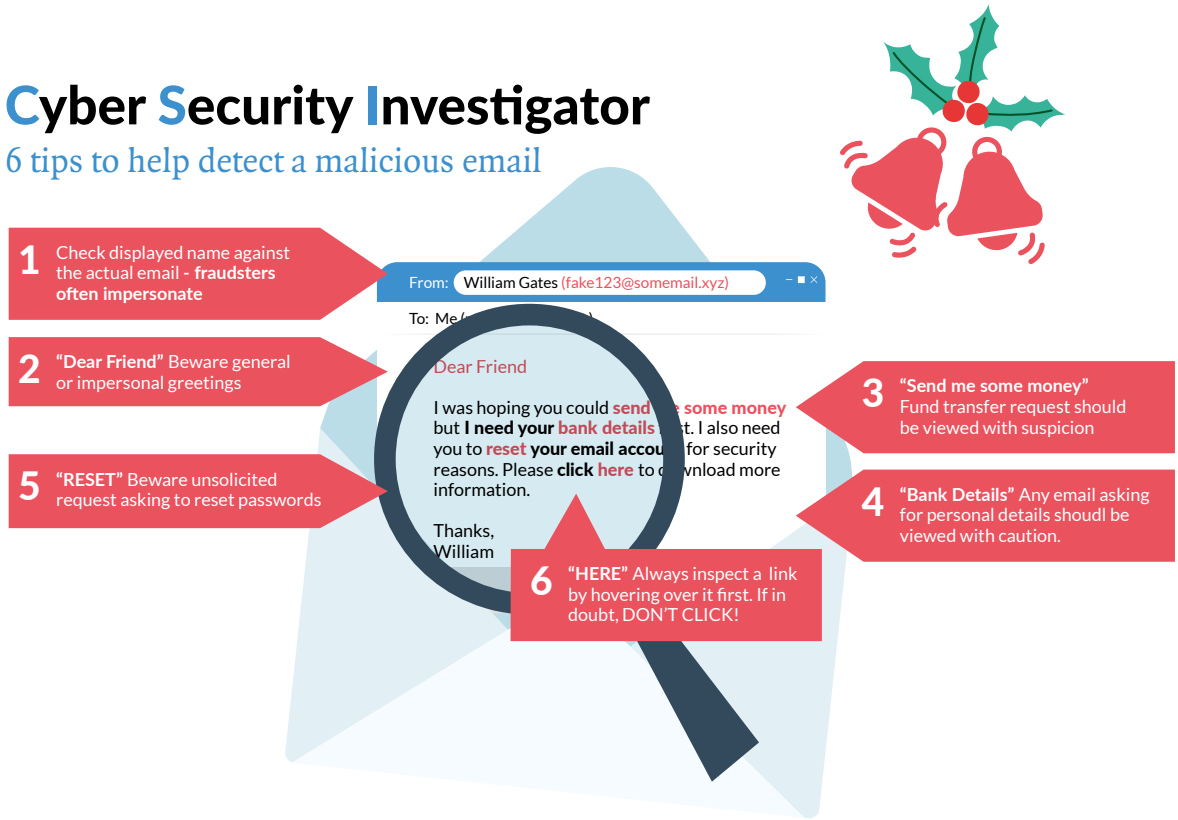


Figure 1: Investigating Suspicious Email

Business Email Compromise

Business Email Compromise (BEC) still remains as one of the most prevalent attack vectors employed by cyber criminals.

During the Christmas period, BEC actors may impersonate a company's CEO or another senior executive in email requests asking a targeted employee to purchase physical gift cards, usually under the guise of staff bonuses or gifts for a client. They will then request the victim to send the code on the voucher to them.

QR Codes

The use of QR codes for fraudulent purposes has also increased and will be prevalent during this busy online shopping period. As new technologies become more mainstream, cyber criminals are often early adopters of these technologies in order to further obfuscate their tactics. These actors will send phishing emails containing a pdf or png image of a QR code which can reduce the possibility of the email being tagged as a phishing attempt. The requirement to scan a QR code increases the likelihood of a recipient to use their personal device outside of an organisations web or anti virus protection.

On scanning the malicious QR code, the recipient is taken to a URL which may be hosting malware or a credential harvesting "sign-in" page. Most modern smart phones will offer a preview of the URL contained within the QR code. Recipients of QR codes should take the time to examine these URLs and assess if the URL looks legitimate and if it's information matches with the sending organisation. Users should also use a reliable app to scan QR codes, the advantage of this is that your device will ask you to confirm the action before the code contained in the QR is executed.

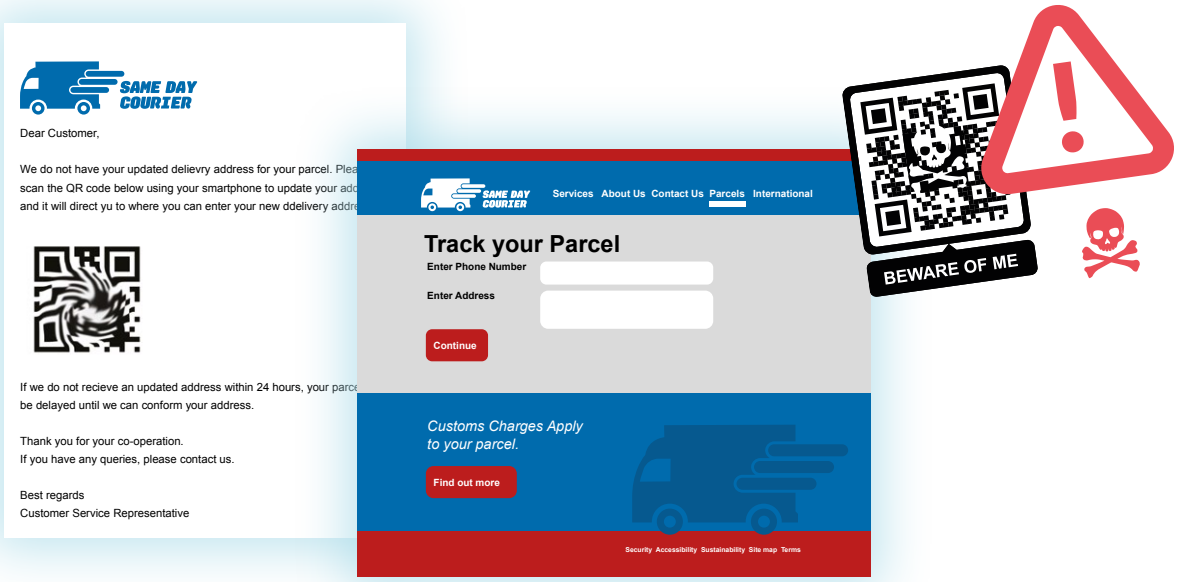


Figure 2: A fake themed website and QR code Phishing attempt

Holiday Scams

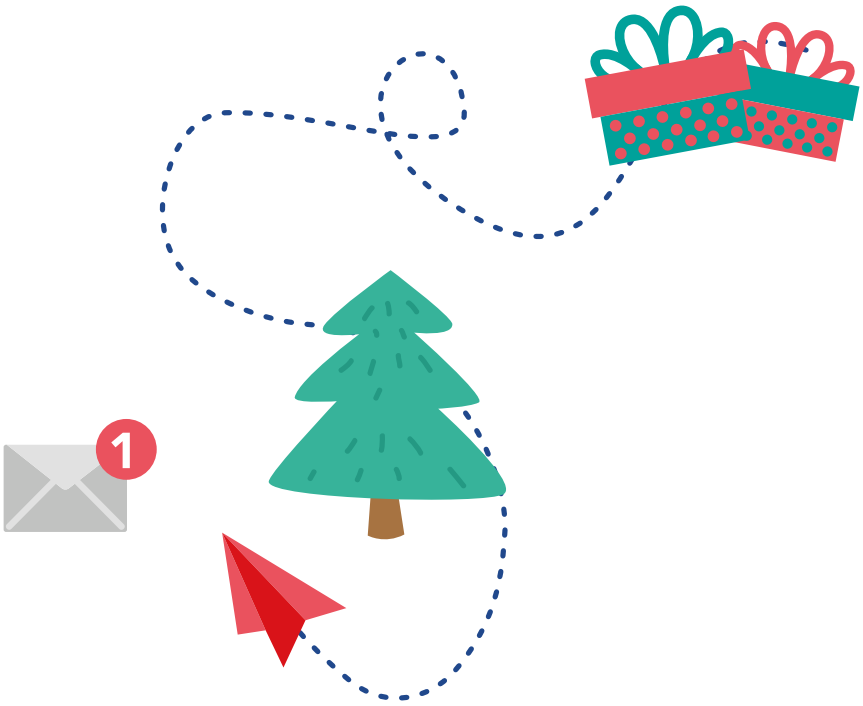
Christmas messages from untrusted sources that ask a user to click a link or play a video/audio file etc. should not be clicked.

Even if the source is trusted, extreme caution should be exercised as the source itself may have been compromised or spoofed. Be particularly vigilant around New Years Eve and Christmas Eve when the volume of messages, both legitimate and malicious, increase greatly.

Holiday makers in Ireland and globally recently reported receiving suspicious emails seemingly originating from a trusted booking website[3]. It is reported that this campaign targeted hotels, booking websites, travel agencies and ultimately their customers. While this was a multi-step, sophisticated attack, potential victims should be aware of the threat posed. If a payment is requested that is not as described within the policies set out by the travel organisation, or if it asks for a payment outside of the parent organisation platform, then people should not continue this payment and should also report this to the parent organisation platform.

It should be noted that even the most advanced threat actors use these methods, particularly at this time of year, to gain unauthorised access to networks, or to steal users' credentials. If you suspect that your details may have been compromised you should:

1. **Contact your bank** or credit card company
2. **Report the crime** to your local Garda station
3. **Reset your login details** for the affected accounts



[3] https://perception-point.io/blog/stealing-more-than-towels-the-new-infostealer-campaign-hitting-hotels-and-travel-agencies/

Staying Secure Online

The NCSC hopes the following security advice can help make your Christmas season a more cyber secure experience.

Before you make any online transactions **research who you are purchasing from** - check online reviews, sales history etc. Preferably use reputable shops and brands you know and trust. If you have any doubts about the seller, we advise you shop somewhere else.

Use a credit card or a virtual credit card when purchasing online.

Never send credit card details by email.

Where possible **type in URLs** to sites you want to visit rather than clicking on links.

Be alert to the existence of fake websites.

- Websites of online retailers can be easily duplicated or "mirrored". This means that afake site can be identical to the original. This means that your payment and order has not been received by the people hosting the impersonated website but the goods will not be shipped. Check the URL when browsing and if in doubt, contact the vendor directly.
- When browsing, make sure each site you visit starts with HTTPS, this indicates that malicious 3rd parties cannot **intercept** any of the details being sent between you and the website you are currently visiting. It should also be noted than most malicious sites will now have valid SSL certificates so **the lock icon is not a guarantee of reputability**. If the website looks poorly designed (spelling mistakes, broken buttons/links etc) use extra caution.

Only install apps from the official App Store or Play-Store and assess the permissions that each app requests in your phone settings

Make sure to **update the device software and applications** to the latest version

Use an ad blocker locally on your browser. These will often block any malicious/unsolicited advertising (malvertising) campaigns that aim to capitalise on shoppers looking for deals

Install reputable anti-virus software on the device

Be wary of unsolicited phone calls claiming to be from banks, internet providers or any other entity requesting passwords, usernames or money for any service. Contact the retailer or service through an alternative contact method to confirm that the request is legitimate.

Invoice re-direction/Business Email Compromise (BEC) fraud is prevalent at this time of the year as businesses are preparing for financial year end. People should be wary of this and enhanced vigilance should be practiced when receiving emails from vendors/clients notifying of a change of bank account and requesting payments made into the new account. Users should verify the change using established alternative forms of communication.

Do not enter your account credentials if you receive an unsolicited email purporting to be an online shipment/delivery company without verifying first. In the event of users wishing to query the status of a particular item they should take note of reference numbers etc. provided at the time of original purchase and ensure these match any subsequent correspondence.

Use caution when connecting to public Wi-Fi.

- Public Wi-Fi is often targeted by malicious actors and used to eavesdrop on unsuspecting users' online activity. We recommend that you use your mobile network if in doubt.
- Never use public Wi-Fi when purchasing online or accessing your bank account.
- The NCSC advises the use of a secure and reputable VPN service if possible.

Create strong complex passwords:

- Passwords should be at least **12 characters** in length.
- Consider using **passphrases**; these are easier to remember and help in creating longer, more complex passwords.
- Use **random and unrelated words**. The greater the complexity the better.
- Use **words that do not appear in the dictionary**.
- Use words from **different languages**.
- Use a **combination of random numerical and special characters** throughout the passphrase.
- **Do not use common phrases** or quotes.
- **Do not use personal words** like family names, pets, local football club or anything associated with your personal life.
- **Do not use words or abbreviations associated with your organisation or industry.**
- Consider using a **password manager.**
- **Do not reuse passwords** across multiple accounts

Secure your devices and accounts:

- **Enable Multi-Factor Authentication (MFA).** Multi-Factor Authentication, also known as MFA or 2FA involves using your username and password and one other piece of information. This other piece of information can come in various forms. It may be:
  > A one time dynamically issued token.
  > A physical object in the possession of the user.
  > A physical characteristic of the user (biometrics).
  > An additional piece of information that is only known to the user.

- **Be wary of MFA Fatigue** - scammers use a strategy in which they bombard victims with 2FA push notifications to trick them into authenticating their login attempts. The account owner is continuously bombarded with prompts asking them to verify their identity which continues until they slip up, are worn down psychologically or the attacker moves on.

Be wary of text messages from shops, charities or delivery companies **requesting you to click on a link or install a new app.**

- **DO NOT** click on the link, never reply to the message, and delete the message immediately.
- Be wary of messages informing of a new voicemail with a link included.

If you have clicked on a link and/or installed an app:

- Perform a factory reset on the device. *(Note: If you do not have backups you will lose data).*
- If you have entered in your bank account details inform your bank immediately.
- Contact your mobile provider for further advice.
- When restoring backups do not restore from any backups created after you installed the malicious app as these will be infected.
- Reset passwords on any accounts used after you installed the app. If you use the same passwords on other accounts, change these also.
- If you have an Android device make sure that the Google Play Protect Service is switched on.

NCSC Guidance
National Cyber Security Centre

FraudSmart Guidance
FraudSmart

Garda Cyber Crime Bureau Guidance
An Garda Síochánna

Europol Tips And Advice To Avoid Becoming A Fraud Victim
Europol

Revenue Guidance
Revenue.ie

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

NCSC
National Cyber Security Centre