NCSC
National Cyber Security Centre

2211231201-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Guide

Seasonal Cyber Awareness
2022-11-24

Status: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Seasonal Awareness

As we approach the Christmas period 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 unauthorised electronic payment fraud (excluding cards) rose to €21.5m, driven by sharp increase in online and mobile banking[1]. The BPFI report also states that card fraudsters stole nearly €45 million through frauds and scams in the second half of 2021, a jump of 50% on the same period last year.

Whilst email phishing is still the most common attack vector for such crimes, smartphones are also targeted through SMS phishing (smishing) and through malicious links embedded in popular messaging & social media apps.

Another attack method used by cyber criminals is fake refund or shipment tracking sites that attempt to harvest credentials (username/passwords/credit card details etc.), from unsuspecting victims. The success of these tactics are based on the increased urgency people feel to track their purchased goods in order for them to arrive in time for Christmas.

Business Email Compromise (BEC) has also increased substantially over recent years. 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.

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.

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 at the very least steal users' credentials. If you suspect that your details may have been compromised you should:

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

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

[1] https://www.fraudsmart.ie/2022/11/21/fraudsters-stole-nearly-e45m-through-frauds-and-scams-in-second-half-of-2021-up-50-on-previous-year-latest-fraudsmart-report/

Staying Secure Online

- 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 a fake site can be identical to the original, but at the last stage they will redirect your payment to different account. This means that your payment and order has not been received by the vendor and 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 many malicious sites will 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. As always, if something appears too good to be true, it probably isn’t true.
- 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.
  - 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

Staying Secure Online (Continued)

- 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.
- 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.
  - 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 malvertising campaigns that aim to capitalise on shoppers looking for deals
  - Install reputable anti-virus software on the device

Staying Secure Online (Continued)

- 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.
- See the following pages for more valuable cyber security tips:
  - NCSC Guidance
  - Garda Cyber Crime Bureau Guidance
  - FraudSmart Guidance
  - Europol Tips And Advice To Avoid Becoming A Fraud Victim

DISCLAIMER: *This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie