

The 12 Scams of Christmas

(Get the warning bells ringing!)

- | | | | |
|--------------------------------|---------------------------------|-------------------------------|--------------------------------|
| 1
Fake
Websites | 2
IT Support
Scams | 3
Fake
Charities | 4
Refund
Scams |
| 5
Phishing
Emails | 6
Gift Card
Scams | 7
Brexit
Scams | 8
Covid19
Scams |
| 9
Phone
Scams | 10
Ecard
Scams | 11
Fake
Romance | 12
Shopping
Scams |



Don't let criminals ruin the festive spirit



[Click here to join!](#)

Swansea Council - Working with Action Fraud, the National Cyber Security Centre and Friends Against Scams

On the 12 days of Christmas, Swansea Gov. said to me

1. Fake Websites

Using the web to buy Christmas presents? Criminals set up fake websites that look identical to steal your personal details and money. Secure website addresses start with “**https**” and display a locked padlock.

2. IT Support Scams

IT support scams could be via a phone call or email stating there is something wrong with your computer and needs fixing. They will try to direct you to a bogus website. Companies like Microsoft will **NEVER** call.

3. Fake Charities

Watch out for criminals using a legitimate charity’s name and appealing on their behalf, for a donation. If suspicious, ask to see their official charity ID which they’re required to carry. **TRUST** your instincts!

4. Refund Scams

You may receive an email or text pretending to be from the Council or a well-known store promising a credit or tax refund and a link to click to claim the money back. They’ll ask for bank details. **DON’T**

5. Phishing Emails

Criminals send emails that look genuine to make you click on a link to a fake site or open an attachment that infects your machine with a virus. They will make you panic and rush your decision. **THINK** before clicking.

6. Gift Card Scams

Received an email from a friend asking to buy gift cards for them? Criminals clone and pretend to be people you know to get you to do this. They are after the code on the card to spend the money. **DON’T**

7. Brexit Scams

Criminals may contact victims to suggest making “No lose” investment to help capitalise on Brexit. They also pose as HM Revenue & Customs to get payments off businesses to register for trading. **DON’T**

8. Covid19 Scams

Received a telephone call from Swansea Council identifying you as a contact of a confirmed case of COVID-19? We will provide advice and ask some personal questions like you address. We **WON’T** ask for financial details.

9. Phone Scams

Criminals ring you to discuss a topic then ask you to press a number on your phone keypad to “opt out” of a survey for example. It will generate extreme charges which the criminals will profit from. **DON’T**

10. Ecard Scams

Watch for those e-cards you receive online. It could be infected with a virus that could shut down your device and you could be held to ransom to restore files. Get an **Anti-virus** installed that will alert you!

11. Fake Romance

Looking for festive love online? Criminals are. The relationship develops over time and the individual is convinced to make payments to the criminal - **DON’T**. They’re also after your identity. Guard your privacy.

12. Shopping Scams

Love top brands with low prices? Well stay vigilant for counterfeit goods. These range from poorly made clothes to dangerous electronics which fail to comply with safety laws. If it sounds **too good to be true**, it probably is.



Reporting and further advice



If you want to report fraud or cybercrime, please contact Action Fraud.

- If you are a victim of a scam, report it to Action Fraud via www.actionfraud.police.uk
- If you are a business, charity or organisation which is suffering a live cyber-attack, call Action Fraud - **0300 123 2040**



If you want more advice and guidance on cyber security, visit the National Cyber Security Centre (NCSC)

Whereas Action Fraud deals with cybercrime reporting, the NCSC is a separate organisation that provides expertise advice and guidance on cyber security to help make the UK the safest place to live and work online. They will help protect you and your family and the technology you rely on.

Cyber security is important because smartphones, computers and the internet are now such a fundamental part of modern life, that it's difficult to imagine how we'd function without them. From online banking and shopping, to email and social media, it's more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data, and devices.

Having problems with any of the following? The NCSC can advise:

- My email account has been hacked. I am worried that my banking details have been stolen.
- I have malware (**Malicious software**) on my device. Should I pay a ransom to unlock my computer?

Visit the NCSC online at <https://www.ncsc.gov.uk>

Worried about an email you have received asking for sensitive information or encouraging you to visit a fake website or threatening you with a fake video they have of you, forward them to the NCSC - report@phishing.gov.uk



Need local advice and guidance?

Swansea Council's trading standards department are here to help our residents and businesses with advice and guidance on scams, doorstep crime, street trading etc. Visit our website: <https://www.swansea.gov.uk/tradingstandards>

