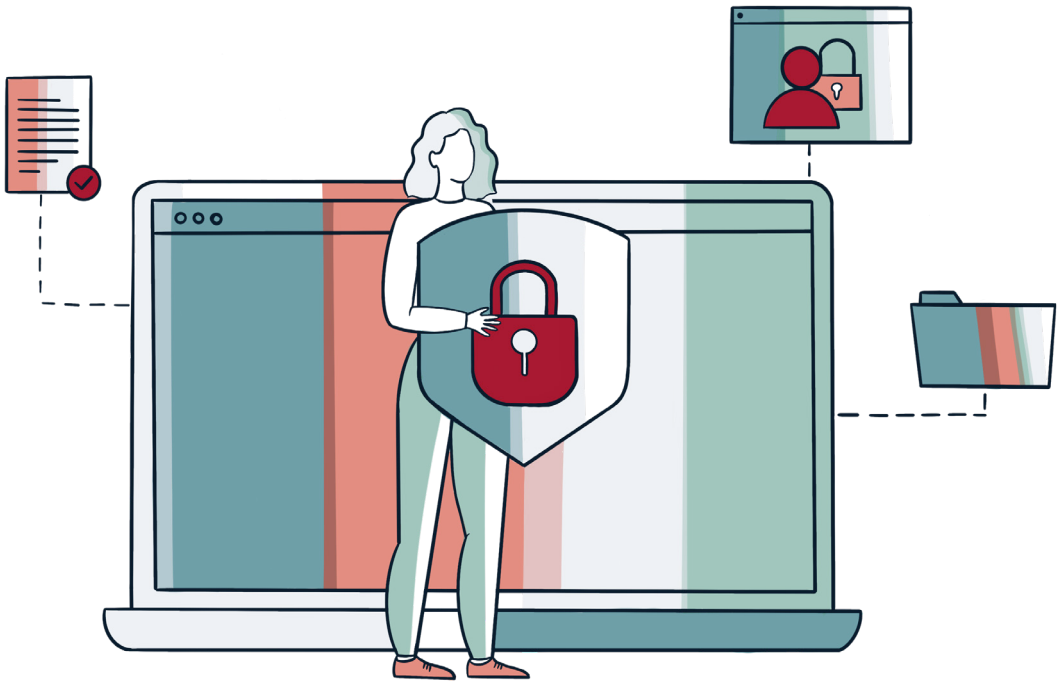
PREVENTING

Identity Theft

Read time: 5 mins



Hello,

Good data protection practices are essential to help reduce the risk of identity theft.

Identity theft happens when fraudsters access enough information about someone's identity, such as their name, date of birth, and current or previous addresses, to commit identity fraud.

Criminals commit identity theft by stealing personal information, such as taking documents from the rubbish or making contact with an individual and pretending to be from a legitimate organisation.

Criminals can then commit identity fraud by using the personal information they have obtained to impersonate the individual.

This guide will explore what identity theft and phishing are and the steps we can all take to protect ourselves and our customers!

This ebook is brought to you by:

Learninglab

Identity Theft

Introduction

Fraudsters can use an individual's identity details to:

- **Open bank accounts.**
- **Obtain credit cards, loans and state benefits.**
- **Order goods in their name.**
- **Take over their existing accounts.**
- **Take out mobile phone contracts.**
- **Obtain genuine documents such as passports and driving licences in their name.**

Being a victim of identity theft can lead to fraud that directly impacts an individual's personal finances. It can make it difficult for an individual to obtain loans, credit cards or a mortgage until the matter is resolved.

It is vitally important that your business has sufficient data protection practices in place to look after your customer's personal details.

Imagine how you would feel if you were a victim of identity fraud as a fraudster was able to obtain your personal data from an organisation who you trusted!

Preventing Identity Theft

As well as ensuring you are protecting your customer's data, don't forget that there are steps you can take to protect your own personal data!

Keep things safe

Don't leave things like bills lying around for others to look at. Keep your personal documents in a safe place, preferably in a lockable drawer or cabinet at home.
At work, do you have a clear desk policy?

Shred it - before you bin it!

Don't throw away entire bills, receipts, credit-or debit-card slips, bank statements or even unwanted post in your name. Destroy unwanted documents, preferably by using a shredder.
At work, do you have a confidential waste process?

Immediately Report Lost or Stolen items

You should report all lost or stolen documents – such as passports, driving licences, plastic cards, chequebooks to the relevant organisation.

Preventing Identity Theft:

Verify and question

Do not give any personal information to organisations or people before verifying their credentials. Never reveal your full password, login details or account numbers. A bank or building society will never ask for your PIN or a whole security number or password.

Online protection

Installing or enabling anti-virus software on your devices will protect them from viruses and hackers. Always install the latest software and app updates on all of your devices.

Are all your IT systems up to date?

Use different passwords

Protect your online accounts with strong, **DIFFERENT** passwords and, where possible, enable two-factor authentication. Using different passwords increases security and makes it less likely that someone could access any other accounts.

Make sure you do the same at work!

Preventing Identity Theft

Who's listening?

When giving your card details or personal information over the phone, internet or in a shop, make sure other people cannot hear or see your personal information.

At Source, we use a mute function when taking customer payment details.

Check your details

Check your statements carefully and report anything suspicious to the bank or financial service provider concerned. You should regularly get a copy of your credit file and check it for entries you don't recognise.

If you spot anything suspicious, make sure your report it!

PREVENTING IDENTITY THEFT:

Phishing

What is phishing?

Overview

Phishing is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Phishing can also involve sending malicious attachments or website links to infect computers or mobile devices.

Criminals send bogus communications emails, letters, instant messages or text messages. Very often, these appear to be authentic communications from legitimate organisations. Embedded links within these messages can direct the recipient to a hoax website where their login or personal details may be requested. The computer or smartphone is also likely to be infected by viruses. Once an individual's details have been accessed, criminals can record this information and use it to steal a person's identity.

Criminals have stepped up their activity by targeting business users by claiming they have specific business knowledge. These may be business-critical issues: customer feedback, requests for information, staffing or legal notices.

Phishing

How to recognise a phishing attempt

1. Don’t click or share

Never automatically click on a link in an unexpected email or text. Email addresses and phone numbers can be faked, so don’t use those as a means to verify that a message or call is authentic.

Phishing emails are sent to a vast number of randomly generated addresses. Clicking embedded links can verify your active email address. Once this occurs, it may facilitate the targeting of further malicious emails. Even “unsubscribe” links can be malicious.

Never give your login or personal details when responding to emails or phone calls.

2. Use the SPAM filter

If you detect a phishing email, mark the message as spam and delete it. This ensures that the message cannot reach your inbox in future.

Phishing

How to recognise a phishing attempt

3. Is it a trusted source?

Phishing messages try to convince the recipient that they are from a trusted source.

"Spear-phishing" is a technique whereby criminals use personal information to earn trust and lower the intended victim's defences increasing the chances they may open attachments or embedded links.

Never respond to a message from an unknown source. Ensure that the email is from a trusted source and that you are subscribed to the service.

Be extremely wary of post, phone calls, emails or ads offering you business deals that sound too good to be true out of the blue. Listen to your instincts - if an offer seems too good to be true, it probably is.

Phishing

How to recognise a phishing attempt

4. How to recognise fake emails

Fraudsters are unlikely to know your real name; therefore, the email may address you in vague terms, for example, 'Dear Valued Customer'.

Phishing emails will probably contain odd 'spe11ings' or 'cApitALs' in the 'subject' box and contain spelling or grammatical errors in the email – this is an attempt to get around spam filters and into your inbox.

Banks and reputable organisations will never send you an email asking you to click on a link and confirm your bank details or pressure you into making a financial transaction.

If something feels wrong, then it's usually right to question it.

CONTROLS @ Source

Preventing Identity Theft

How Source protects you and your customers

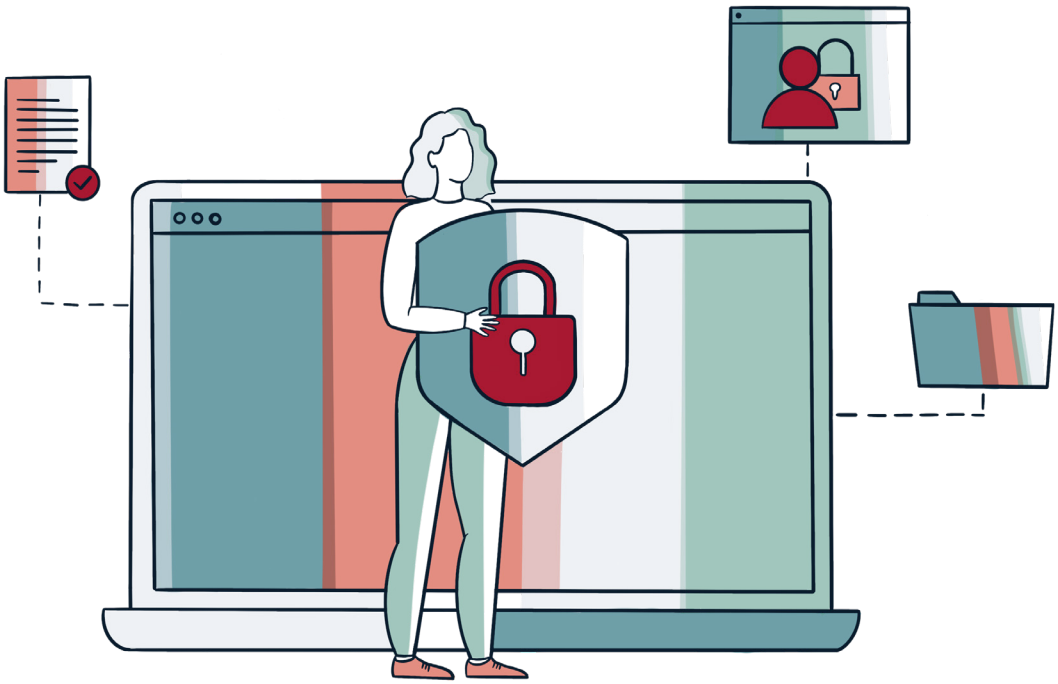
Here are the day-to-day activities that Source has put in place to assist in keeping your and your client's data secure:

Security questions

- Our security questions are in place to identify our policyholders or brokers every time they contact us or if we need to call them.
- On each call, we make sure that we speak to the person entitled to this information.
- By following our processes, we protect the policyholder's data against misuse and handle it appropriately.

Clear desk policy

- All outstanding departmental work is placed in a closed/locked cupboard each evening.
- Nothing is left on printers overnight.
- All outstanding personal work is placed in a closed drawer.
- All paper with scribbled notes is put into confidential waste or filed with outstanding personal work.
- All of the main desk space will be clear.



Source™

Your Property Insurance Experts