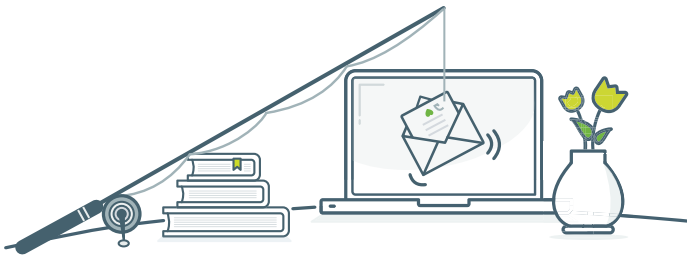
LV= BROKER

Watch out for insurance ‘Vishers’!

What is ‘Vishing’?

Vishing is the criminal practice of using psychological manipulation to obtain sensitive information over the phone. Fraudsters make vishing calls to illegally obtain information, such as details of our customers or claims. They will often pretend to be someone else, suppliers, other insurers or solicitors. Often these vishers will try to entice customers to submit a claim.



What technology is used to make a ‘Vishing’ call?

- **Caller ID Spoofing**: This is the practice of causing the telephone network to display a false number on the recipient’s caller ID. These tools are typically used to populate the caller ID with a specific company to legitimise the call.
- **Hot key transfer** – Vishers sometimes transfer policyholder’s call over, but stay on the line and listen to the remainder of the call, looking to obtain further information.

Here are some of the ways you can spot a ‘Visher’ on the line...

- The caller has partial or incorrect information.
- Background noise might indicate the caller is in a business or call-centre.
- The caller entices you into a friendly conversation.
- A caller impersonating a policyholder may have a voice that does not match the demographics of the customer.
- The caller is not a party on the claim, e.g. when a supplier is impersonated.

How to handle a ‘Visher’

If you think you’re speaking with a ‘Visher’, consider:

- Requesting further information, e.g. asking questions about the policy, asking why the ‘Visher’ requires that information.
- Asking for the caller to contact you in writing.
- For customer impersonations, offer to call the customer back on the telephone number you have on file.
- Request claimant representatives provide a signed mandate of authority.

If you receive a suspected vishing call, always make sure to follow your company’s vishing strategy.

0032798-2021