<https://www.moneyhelper.org.uk/en/money-troubles/scams/a-beginners-guide-to-scams>

* **Unsolicited or unexpected contact** • If you’ve received any kind of contact, but particularly a phone call, out of the blue, it is best to avoid it. Since January 2019, there has been a ban on cold calling about pensions. This means you should not be contacted by any company about your pension unless you’ve asked them to.
* **Email address** • If you get an email, expand the pane at the top of the message and see exactly who it has come from, it could say it’s from TV Licensing but if you click or hover over the name it might reveal something different. If it’s a scam, the email address the message has come from might not match up with the sender’s name, have misspellings, random numbers or be from one of your contacts that’s been hacked.
* **Text messages** • Modern scammers can make their numbers look like one you trust, like your bank’s. The scam text message might even appear in the same conversation as legitimate texts you’ve had before. This is known as ‘number spoofing’. Just in case, avoid clicking links in text messages, and don’t be afraid to contact the company directly to check it’s a real message.
* **If it sounds too good to be true, it usually is** • This is something you normally find with pension or investment scams, where the fraudster guarantees you huge returns, but tells you it is low risk.
* **Personal details, full PIN codes and passwords** • These are things no legitimate company will ask you for.
* **Quick decisions** • If you are pushed into making a decision on the spot, be suspicious. Scammers don’t want you to have time to think about it. Any legitimate company who calls you won’t mind if you hang up and call them back later. Use the phone number you find on letters from the company or the back of your card.
* **Random competitions** • Particularly if you don’t remember entering them, should ring alarm bells.

<https://clario.co/blog/get-revenge-on-spam-email-scammers/>

How to scam a scammer

**2. Scambaiting:** You can try to engage the scammer, emailing them back and pretending to play along with whatever scam they’ve concocted. Because you’re simply replying to an email the scammer sent you, there is little to no chance of getting into any legal trouble. Many individuals, such as Kitboga above, specialize in scambaiting and have made a profession of it.

If you choose to go down this route, you may want to use a dummy email account when pretending to play along. This would make it much harder for a scammer to link you to your actual email, minimizing the chance of any fallout. If the scammer does retaliate by flooding your dummy email account, simply close it and start over with a new one.

**3. Join Forces With Others:** There are a number of online communities, such as [419eater.com](https://www.419eater.com/), that specialize in helping scambaiters collaborate, warn each other and team up to scambait the scammers.

<https://nl.wikipedia.org/wiki/Scambaiting>

Scambaiting kan in categorieën worden onderverdeeld:

1. Straight bait: e-mail tussen de oplichter en de scambaiter.
2. Phone bait: zorgen dat de oplichter de scambaiter opbelt.
3. Church bait: zorgt dat de oplichter toetreedt tot de scambaiter zijn kerk.
4. Safari bait: zorgen dat de oplichter reist.
5. Art bait: zorgen dat de oplichter iets van kunst maakt.
6. Cash bait: een illegale actie om geld te winnen van de oplichter.
7. Freight bait: zorgen dat de oplichter betaalt voor de verzendingskosten van iets kostbaar voor de scambaiter.

<https://www.theguardian.com/technology/2021/oct/03/who-scams-the-scammers-meet-the-amateur-scambaiters-taking-on-the-crooks>

**T**hree to four days a week, for one or two hours at a time, [Rosie Okumura](https://www.youtube.com/user/rosieokumura), 35, telephones thieves and messes with their minds. For the past two years, the LA-based voice actor has run a sort of reverse call centre, deliberately ringing the people most of us hang up on – scammers who pose as tax agencies or tech-support companies or inform you that you’ve recently been in a car accident you somehow don’t recall. When Okumura gets a scammer on the line, she will pretend to be an old lady, or a six-year-old girl, or do an uncanny impression of Apple’s virtual assistant Siri. Once, she successfully fooled a fake customer service representative into believing that she was Britney Spears. “I waste their time,” she explains, “and now they’re not stealing from someone’s grandma.”