PRESS RELEASE

Amazon scam ‘on the rise’ warns Lloyds Bank

- **‘Remote access takeover’ sees scammers trick victims into handing over control of their device**
- **Fraudsters’ attempts at this scam have more than doubled over the last 12 months**
- **Resurgence seen in ‘Amazon’ version of the scam which first came to the fore last year**

People need to be on their guard against computer takeover scams this summer, according to Lloyds Bank.

The scam usually happens when the victim receives a phone call. Fraudsters pretend to be from a trusted company and may offer a refund or help with a fault or a problem. But to help, they need to take ‘remote control’ of your device.

Attempts at this type of fraud have more than doubled over the last year – and right now fraudsters are using Amazon as part of their cover story. This is a version of the scam which first came to the fore during lockdown last year, with fraudsters thought to be taking advantage of the higher number of people shopping online, as well as more people sharing their screens during video calls.

Here’s how it works

- A call out of the blue that claims to be from Amazon and offers a refund, or help with a fault or problem.
- The caller may know details about your account. And the phone number could look genuine as fraudsters can easily copy or ‘spoof’ telephone numbers.
- They ask you to download a tool, such as TeamViewer or Quick Assist. They say this will give them remote control of your device so they can pay you the refund.
- Then they ask you to log on to your online bank account to get the refund.
- At this point, they could take control of your online bank account without you knowing.
- The caller might give you a code to put into an automated bank call to get the refund.
- This code has nothing to do with a refund. It’s to approve a payment to someone new that the fraudster has set up on your bank account.

This scam often begins much earlier than the first phone call. Fraudsters send emails or texts to try to get personal details from people. These scam messages often pretend to be from a well-known company or organisation, such as Royal Mail or HMRC. They include a link to a fake website that asks for personal or banking details. Once a fraudster has these details, they can use them to make a scam call and gain a person’s trust.

Philip Robinson, Retail Fraud Prevention Director at Lloyds Bank, said: “Organised criminal gangs are forever inventing new ways to dupe unsuspecting victims out of their money, but they’re always ready to re-use tactics that have worked for them before, hoping that people have forgotten previous warnings.

“We’ve seen a big spike in attempts recently where fraudsters convince people they’re from big trusted retailers and to download software onto their device. Once they have access to a victim’s computer, tablet or phone, it opens up a treasure trove of personal information and sometimes even access to bank accounts.

“Fortunately, we’re able to stop many of these scammers in their tracks with sophisticated monitoring of our customers’ online banking accounts. But sadly, the fraudsters only need to be successful once to make off with thousands of pounds of someone’s hard-earned cash, which can leave a devastating impact.

“That’s why we want people to stay alert to the threat of this scam. Be wary of any messages you receive which you weren’t expecting, and don’t click on links in emails or texts. If you receive a call out of the blue, never download software or make a payment because someone asks you to, even if it seems they already know all about you and are trying to help. Always hang up and report it to your bank immediately.”

How to avoid this scam

1. **Click with care** - Only click on a link in an email or text if you know and trust the sender.
2. **Hang up** - If you’re not sure who’s calling, put down the phone.
3. **Call to check** - Use a number you trust, not one a caller uses or may give you.
4. **Download with care** - Never download anything to your device for a call out of the blue.
5. **Keep your details private** - Never share your personal or banking details.
6. **Protect your account** - Never log on to your online bank account for someone who calls.

Media contacts

Gregor Low
07500 078879
Gregor.low@lloydsbanking.com

Kimberley Hamilton
07557 257 298
Kimberley.hamilton@lloydsbanking.com

Follow us

@LloydsBankNews