

All about fake emails, fake calls and messages



Scammers are **people** that **steal** from **others**. **Scammers** use **fake** phone **calls**, **messages**, or **emails** to **steal** from **people**.



The phone **calls**, **messages** or **emails** can **look like** they are from your **bank** or from other **well-known places**.



The **fake messages**, **emails** or phone **calls** can **look** very **real** to **trick people** into **giving** important **details like** their **passwords** or **bank card numbers**.



For example, **scammers** send a **fake message** saying that you **need** to **pay** for your **parcel** to be **delivered**. You **paid** because the **message** looked **real**.



Giving a **scammer** your **information** or **money** because of a **fake call**, **message** or **email** is called a **phishing attack**.



This **Easy Read** will **tell** you **some ways** to to **stay safe** from **scammers** and **phishing attacks**.

Staying safe from fake emails



When you **get** an **email** from your **bank** **asking** for your **details** or to **pay something**, it is always **best** to **be careful**.



Sometimes **fake emails** can **have** a **phone number** for you to call. This **number can be fake**.

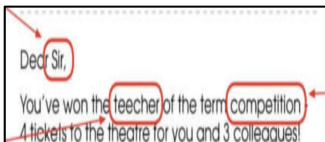


It is **better** to **find** your **bank number** on **Google** and **call** the **real number** to **check** if the **email is real**.

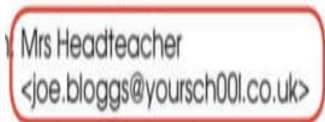
Ways to spot fake emails



Look at the **email address**. **Fake emails** will have **strange-looking email** addresses.



Some fake email addresses might **have misspellings** or extra characters.

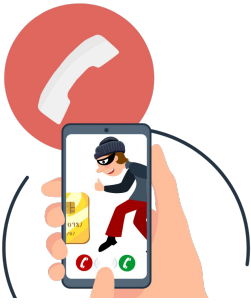


For **example**, an **email** from **Paypal** that **looks strange** like "supp0rt@paypal.com". This email has the number "0" instead of the letter "o".



Many times, fake emails start without your name. For example **with** "**Dear customer**" or "**Dear user**"

Staying safe from fake phone calls and messages



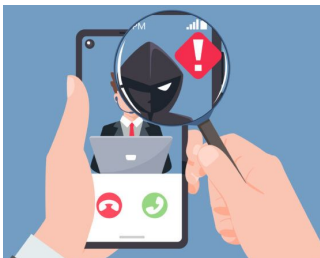
Do not answer phone calls from **strange numbers** that you are **not expecting**.



Sometimes, your **phone** will **tell you** that the **phone call** is **from** a **scammer**, with a **message** that **says** '**suspected scam**'. Please **do not answer these** phone **calls**.



When you **get** a phone **call** from a **strange** number, you can **search** the **number** on **Google**.



Searching a **strange** phone **number** can **help** you **see** when the **number** is **from** a **scammer**.



There is a **website** called "**who called me?**" that **lets people check** if a **phone number** is **real** or a **scam**.



Just type the **website address** on the **searching** bar. The **website is:**

www.who-called.co.uk

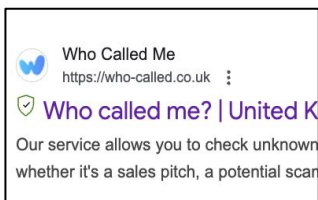
How to check phone numbers online



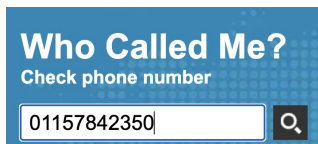
1- Open google



2- Type "who called me?"



3- Click on the "who called me" page



4- Type the **number** on the **page** and **press enter**



5- See what the **page** says about the phone number.



When it says "**Negative**" in **red**, that means the **call** could **be from** a **scam number**.



Always ask someone you **trust** for **help** when you are **not sure** about something!



Now you know a lot more about phishing attacks - fake messages, fake emails and fake phone calls.

Do you **want** to **join us** and learn more about Makaton and inclusive communication?



Just email info@include.org or connect on social media.

You **can** also **call us on 07918470190.**



To **learn more** about the **ways helping others helps you**, read this Easy Read [here](#).



You can also **learn more** about Include's Champions group [here](#) and all about Stroll and Sign [here](#).



Find these Easy Reads and others on our website at www.include.org.