What is a data breach?

A data breach occurs when information held by an organization is stolen or accessed without authorization.

Criminals can then use this information when creating phishing messages (such as emails and texts) so that they appear legitimate. The message has been designed to make it sound like you're being individually targeted, when in reality the criminals are sending out millions of these scam messages. Criminals may even send messages pretending to be from an organization that has suffered a recent data breach.

Even if your details are not stolen in the data breach, the criminals will exploit high profile breaches to try and trick people into clicking on scam messages.

How might you be affected?

In a typical scam, you might receive a message claiming to be from an organization that has suffered a recent data breach. The message could ask you to log in and verify your account because 'fraudulent activity has taken place', or similar.

These scam messages will typically contain links to websites that look genuine, but which store your real details once you've typed them in. Or these websites could install viruses onto your computer or steal any passwords you enter.

Like many phishing scams, these scam messages are hard to spot, and are preying on real-world concerns (in this case, a data breach) to try and trick you into clicking.

And it's not just emails or texts. If the information stolen during the breach includes phone numbers, you might receive a suspicious call. The approach may be more direct, asking you for sensitive information (such as banking details or passwords), or access to your computer.

Actions to take following a breach.

If you're a customer of an organization that has suffered a data breach, you should take the following actions.

1. Find out if you've been affected by contacting the organization using their official website, or email. The organization should be able to confirm:

- if a breach occurred
- how you're affected
- what else you need to do

You can also phone the organization directly but be aware that many won't have the capacity to respond to all calls during a major breach.

2. Be alert to suspicious messages (we've published guidance that can help you with this), which may be sent some time **after** the breach is made public. Remember, your bank (or any other official organization) will never ask you to supply personal information. Things to look out for include:

- official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries.'
- emails full of 'tech speak', designed to sound more convincing.
- being urged to act immediately or within a limited timeframe.

3. If you receive a suspicious message that includes a password you've used in the past, don't panic:

- if this is a password that you still use, you should change it as soon as you can (avoid clicking on any link sent to you)
- if any of your other accounts use the same password, you should change them as well.
- for advice on creating strong passwords and protecting them visit Choosing and Protecting Passwords by CISA.

4. Check your online accounts to confirm there's been no unauthorized activity. Things to look out for include:

- being unable to log into your accounts.
- changes to your security settings.
- messages or notifications sent from your account that you don't recognize.
- logins or attempted logins from strange locations or at unusual times

5. To check if your details have appeared in any other public data breaches, there are a number of online tools that you can use, such as https://haveibeenpwned.com. Similar services are often included in antivirus or password manager tools that you may already be using.

6. To report a cyber security incident including Phishing Scam, Identity Theft, or Online Crime, use the America's Cyber Defense Agency tool.