Microsoft

Think for a tick before you click!

Hackers disguise phishing links and scam ads as credible sources to trick you into clicking on them.

Hackers use bad links to find a way into your devices, such as your...

- Tablet
- Phone
- Computer

When they get in, they can...

- Spy on you
- Access your camera
- Crash your device
- Steal your info

...and more

Bad links can come in...

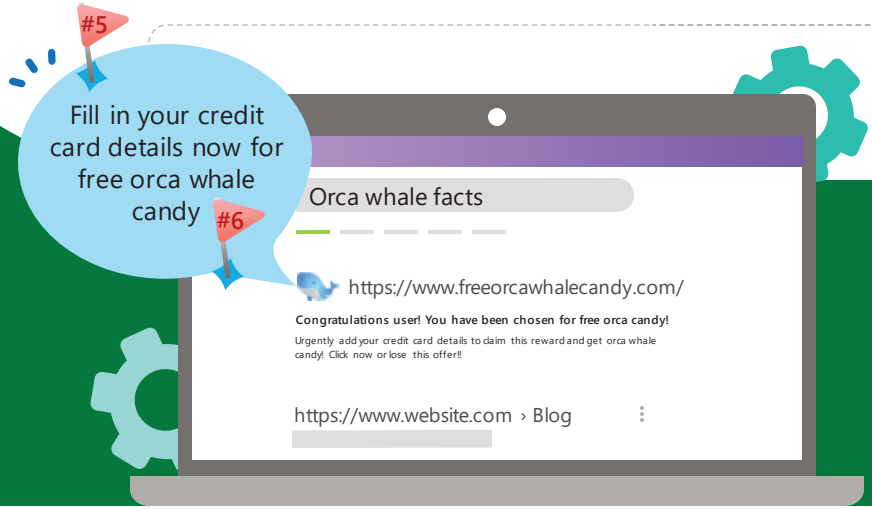
- Websites
- Search engines
- Text messages
- Emails
- Social media posts
- Direct messages (DMs)

Protect yourself with good cyber hygiene!

Look for these common phishing red flags

What is phishing? The act of using fake messages or dangerous links to try and steal your information!

- #1 Misspellings or errors in the message text
- #2 Wrong or suspicious contact info
- #3 Link (or sender's email) does not go where you would expect
- #4 Message conveys threat and urgency
- #5 Asks you to provide private information
- #6 Bargains & offers unrealistic rewards



Not all unknown links are phishing attempts... They could also be scam ads.

How can you identify a scam ad?

- Scam ads can be made to look like real ads, so don't assume they are legitimate just because they have an "**Ad**" or "**Sponsored**" tag
- It may have similar red flags to a phishing message, such as asking for personal data and offering you rewards in exchange

Phishing links are sent to you, while **scam ads** are dangerous links you stumble upon.

If you receive or open a strange link, here's what you can do:

- Don't try to fix it yourself!
- Immediately tell a parent, guardian, or teacher.