Cheat Sheet: How to Spot a Scam Email

Scam emails can look real — but there are always warning signs. Use this cheat sheet to help yourself or a loved one stay safe online. If in doubt, don't click or reply!

🚨 1. Watch the Subject Line

- "Urgent Action Required!"; "Your account has been suspended"; - "You've won a gift card!"

👀 2. Look Closely at the Sender

- Check the email address (not just the name!)
- Scammers often use lookalike domains: e.g., support@micr0soft-help.com

🔗 3. Hover Over Links (Don't Click!)

- Hover your mouse over links to see where they really go
- If the web address looks strange or doesn't match the company, it's likely a scam

💬 4. Bad Grammar or Strange Language

- Many scam emails contain odd wording, typos, or robotic language
- Real companies usually have polished writing

🔐 5. Requests for Personal Information

- Banks and legitimate companies **will never** ask for passwords or Social Security numbers by email
- Don't reply or click forms asking for personal details

🧾 6. Unfamiliar Attachments or Downloads

- Never open unexpected attachments, even if it looks like it's from someone you know
- These can contain viruses or ransomware

☑ When In Doubt...

- Don't click! Call the company using the number on their website
- Forward the email to someone you trust (like SafeClickers!)
- Mark it as spam and delete it