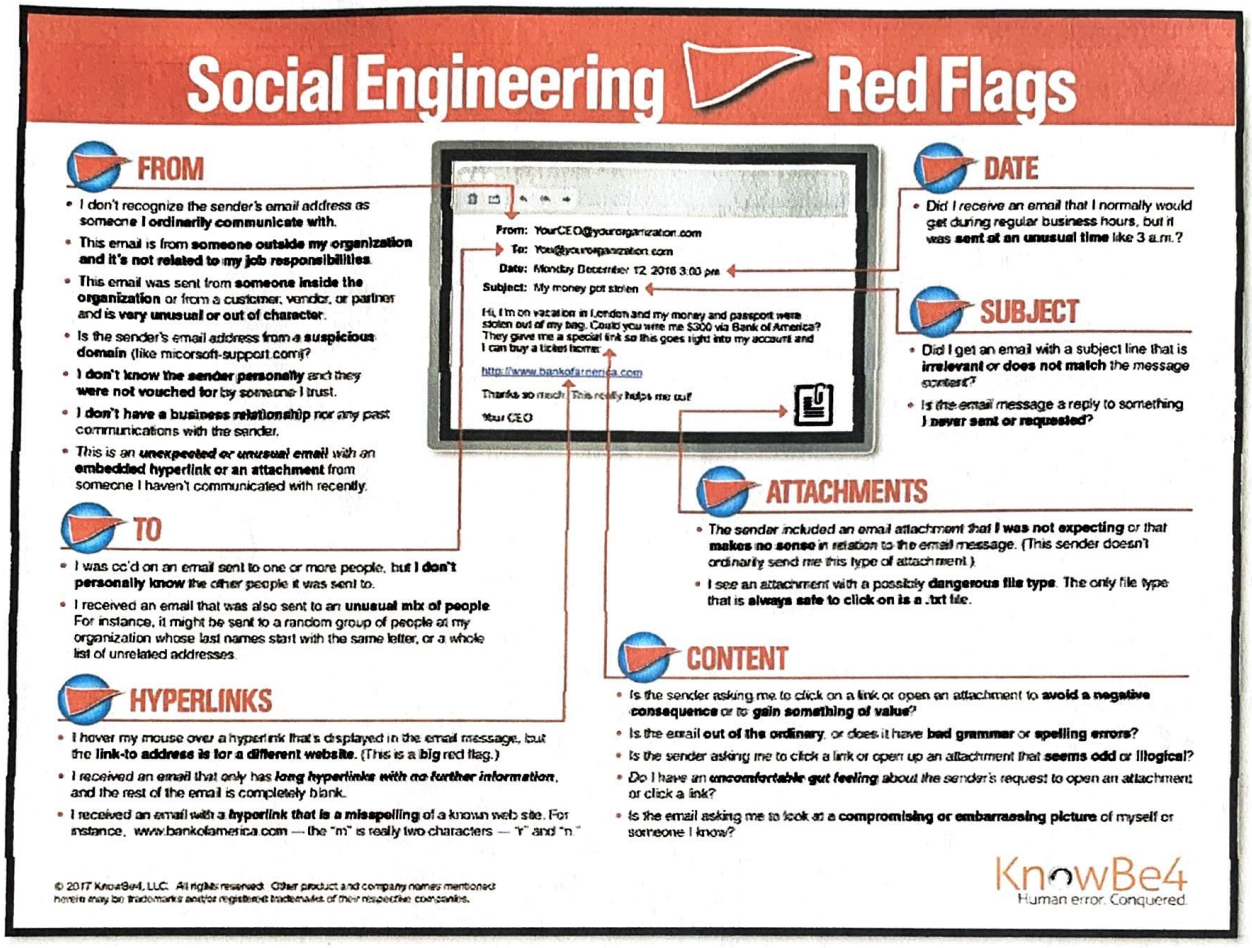
Here is a great KnowBe4 resource that outlines 22 social engineering red flags commonly seen in phishing emails. We recommend printing out this PDF to pass along to family, friends, and coworkers.

Traute
le 25.4.




## Prevent Phishing Attacks:

Though hackers are constantly coming up with new techniques, there are some things that you can do to protect yourself and your organization:

- To protect against spam mails, spam filters can be used. Generally, the filters assess the origin of the message, the software used to send the message, and the appearance of the message to determine if it's spam. Occasionally, spam filters may even block emails from legitimate sources, so it isn't always 100% accurate.
- The browser settings should be changed to prevent fraudulent websites from opening. Browsers keep a list of fake websites and when you try to access the website, the address is blocked or an alert message is shown. The settings of the browser should only allow reliable websites to open up.
- Many websites require users to enter login information while the user image is displayed. This type of system may be open to security attacks. One way to ensure security is to change passwords on a regular basis, and never use the same password for multiple accounts. It's also a good idea for websites to use a CAPTCHA system for added security.