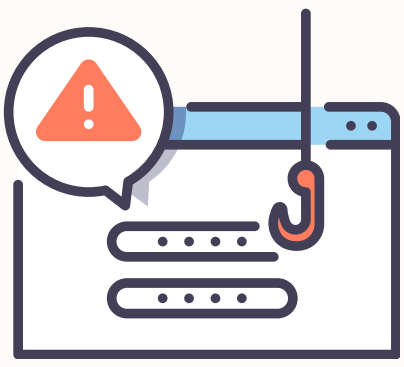
IDENTIFY PHISHING



SIMPLE TIPS WITH A HUGE IMPACT

THE EMAIL ASKS FOR PERSONAL INFORMATION

THEY MAY REQUEST CREDIT CARD INFORMATION, BANKING DETAILS, OR LOGIN CREDENTIALS.

Do not reply or click any links and do not use any communication method provided in the email.

BEWARE OF SUSPICIOUS LOOKING EMAIL ADDRESSES

TAKE A MOMENT TO EXAMINE THE EMAIL ADDRESS AND YOU MAY FIND A SUSPICIOUS VARIATION

For example:

✗ **@state.nm.work** ✓ **@state.nm.us**

IT´S POORLY WRITTEN

CHECK FOR SPELLING ERRORS AND GRAMMATICAL MISTAKES

Emails from legitimate companies will have been constructed by professional writers and exhaustively checked for spelling and grammar.

WATCH OUT FOR SUSPICIOUS ATTACHMENTS

SCAN BEFORE DOWNLOADING

The attachment could contain a malicious URL or trojan, leading to the installation of a virus or malware on your PC or network.

KEEP CALM

THE EMAIL MAY CLAIM THAT YOUR ACCOUNT HAS BEEN COMPROMISED

It might state that your account will be closed if you do not act immediately. If you're unsure, contact the company through other methods.

If an email you receive from the Educational Retirement Board or a group claiming to represent us makes you feel suspicious please contact us immediately.

ERB

Phone: 1-866-691-2345
email: member.help@state.nm.us

SOURCE: WWW.STAYSAFEONLINE.ORG