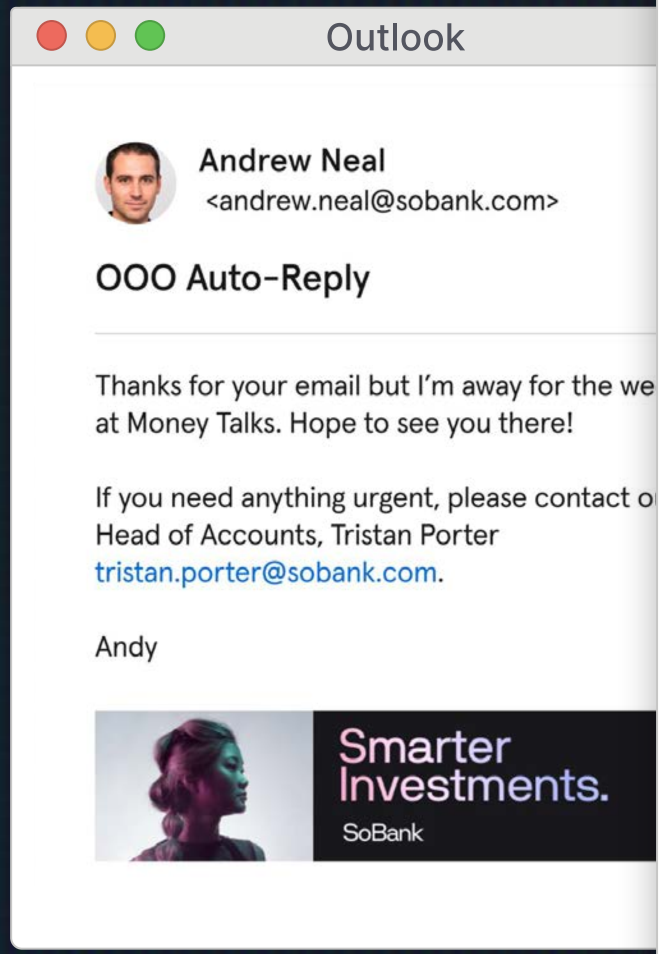
TESSIAN

//how to hack a human

Hackers use the information you post on social media and even on your OOO message to craft targeted – and effective – spear phishing attacks. Use this list of do's and don'ts to help you protect yourself and your colleagues.

Looking for more tips? Ask your security or IT team.

They're there to help!



Andrew Neal
<andrew.neal@sobank.com>

OOO Auto-Reply

Thanks for your email but I'm away for the we
at Money Talks. Hope to see you there!

If you need anything urgent, please contact o
Head of Accounts, Tristan Porter
tristan.porter@sobank.com.

Andy

Cybersecurity Best Practice_Do's.doc

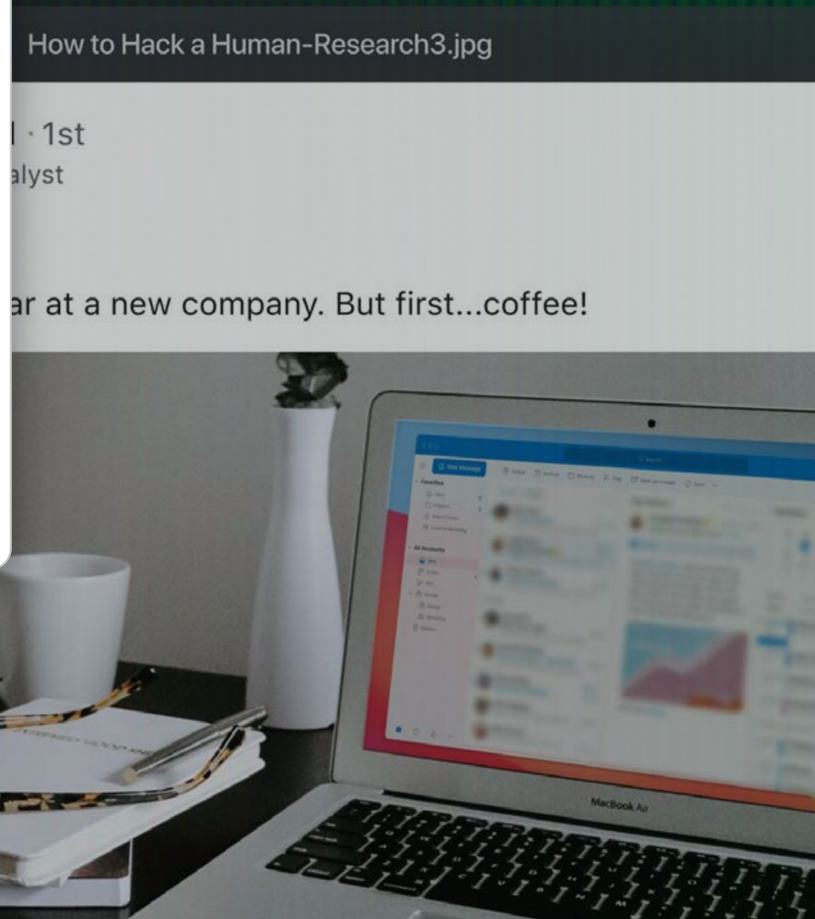
✓ Do

- □ Review your privacy settings on all your social media profiles. Be aware that some will share your information *beyond* the platform.
- □ Configure your OOO settings so that your message is only sent to contacts or email addresses from *within your organization.*
- □ Use strong passwords that don't include your name, birth date, pet's name, or other information that's easy to find online. Better yet, use a password manager like 1Password to randomly generate impossible–to–hack passwords.
- □ Enable 2FA or MFA.
- □ When reading emails, check that the sender's display name and email address match, *especially* if you're on your mobile.
- □ Follow in–house security policies around payment verification before actioning any requests made via email.
- □ Hover over links before clicking on them. If the URL looks suspicious, don't click.
- □ Report anything suspicious! Your security team is there to help.

Cybersecurity Best Practice_Do's.doc

✗ Don't

- □ Re–use passwords for professional **or personal accounts.**
- □ Include too much information in an OOO message. The date of your return is sufficient for anyone outside of your organization. Want to be proactive? **Email customers/clients directly before you log off with relevant contact details for you or a colleague.**
- □ Open attachments or links from senders you don't recognize.
- □ Post photos of your employee ID *or* screenshots of your laptop with work "stuff" visible. For example, your email, your desktop, Zoom Meeting IDs, browser bookmarks etc.
- □ Be afraid to ask for a second opinion about a suspicious message.
- □ Assume that phishing emails are poorly crafted or riddled with grammatical errors. Remember, these are sophisticated attacks designed to look exactly like the real thing.



· 1st
alyst

ar at a new company. But first...coffee!

LEARN MORE ABOUT YOUR DIGITAL FOOTPRINT →