BLACKCLOAK®

Social Engineering Red Flags

Scams and hackers use convincing stories to frame a situation, rush you into making a decision, and heighten your emotions in order to trick and defraud you. Here's some common scams and some tips to recognize their schemes before you get scammed:

Immediate Red Flags

- Anything that involves a gift card.
- Anything that involves sending money via Western Union.
- Anything where someone is offering a refund.
- Anything that requires someone to gain access to your computer by downloading a screen sharing tool. (please see below for a list of these)
- Anyone claiming to be from the government or the IRS.
- Text messages that read "Hi" or look like the sender may have accidentally sent the message to you.
- Anyone claiming to have a family member or that a family member is in an accident, hospital or jail AND needs money sent to them.

Common Scams

- Your friend sends a weird message asking you to look at a picture or view some content on another website that asks for your credentials.
- Someone who initiated contact with you is trying to get you to download software, especially software like TeamViewer, AnyDesk, and similar software that allows remote access.
- A company reaches out to and asks you to click a link or button and update, check, or verify your account information.
- A service company reaches out to you asking you to renew or confirming a renewal, but you don't recall having a subscription to this service.
- When someone needs gift cards from you (for any reason).
- When your emotions get heightened, you are more likely to succumb to a scam.
- If the request is urgent, your judgment can be rushed and taken advantage of.
- If the offer is too good to be true, it often is.
- You're receiving help you may not have asked for.
- If you aren't able to verify the identity of the person sending it.

Where to look

Sender

- I don't recognize the sender's email address as someone I ordinarily communicate with.
- This email is from someone outside my organization and it's not related to my job responsibilities.
- This email was sent from someone I know or from a customer, service provider, or partner and is very unusual or out of character.
- Is the sender's email address from a suspicious domain (like micorsoft-support.com)?
- I don't know the sender personally and no one I know has vouched for them.
- I don't have any past communications or well-known history with the sender.
- This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I am not expecting communication from or have not communicated with recently.

Recipient

- I was cc'd on an email sent to one or more people, but I don't personally know the other people it was sent to.
- I received an email that was also sent to an unusual mix of people. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

Do not click the link in an unsolicited text message or email that asks you to update, check, or verify your account information.

Links + Hyperlinks

- I hover my mouse over a hyperlink that's displayed in the email message, but the link-to address is for a different website. (This is a big red flag.)
- I received an email that only has long hyperlinks with no further information, and the rest of the email is completely blank.
- I received an email with a hyperlink that is a misspelling of a known web site. For instance, www.bankofarnerica.com – the "m" is really two characters – "r" and "n."

Date

- Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.?

Subject

- Did I get an email with a subject line that is irrelevant or does not match the message content?
- Is the email message a reply to something I never sent or requested?

Attachments

- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly dangerous file type.

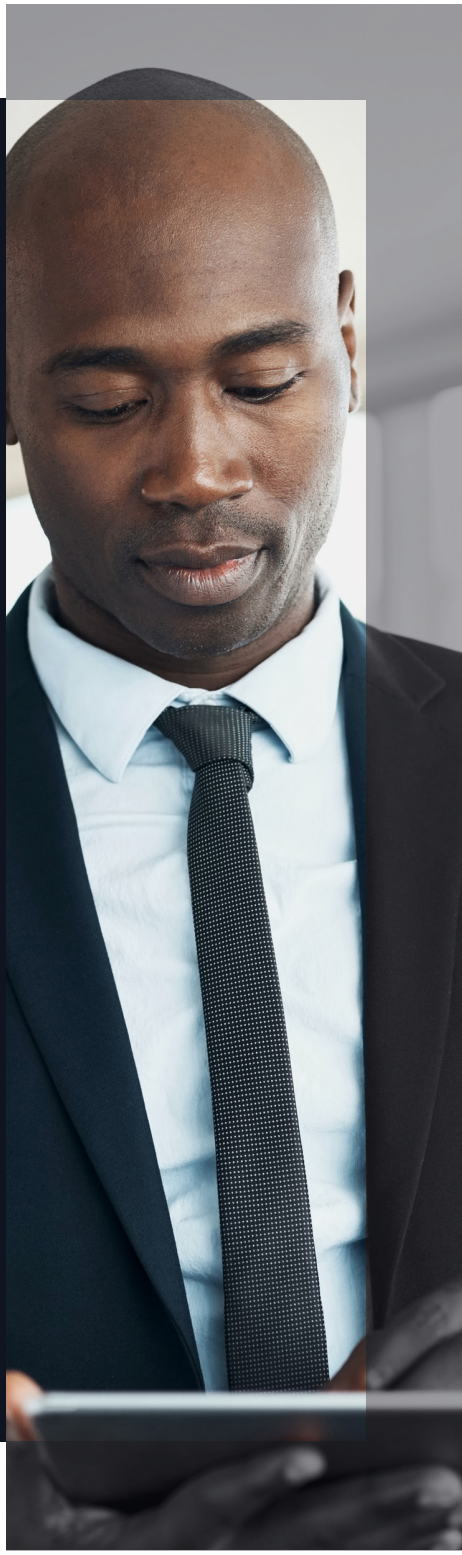
Content

- Is the sender asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?
- Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- Is the sender asking me to click a link or open up an attachment that seems odd or illogical?
- Do I have an uncomfortable gut feeling about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?
- Are you being asked to renew a service (Norton, McAfee) that you don't recall paying for?

BLACKCLOAK®

Combatting Smishing: Tips to Be Mindful of

Dealing with smishing can seem daunting, but there are practical measures you can take to protect yourself.



Be wary of unknown numbers and senders:
Be cautious if you receive a text message from an unfamiliar number or person. Avoid clicking on any embedded links or dialing numbers included in the message.

Avoid calling back:
If a message instructs you to reach a specific number, resist the urge. Scammers often use this technique to further their deceit.

Delete suspicious messages:
The best action upon receiving a suspected smishing message is to delete it, as this ensures you won't inadvertently click on harmful links later.

Use your phone's spam features:
Modern smartphones have built-in features that allow you to block spam messages or specific numbers. Make sure to take full advantage of these capabilities.

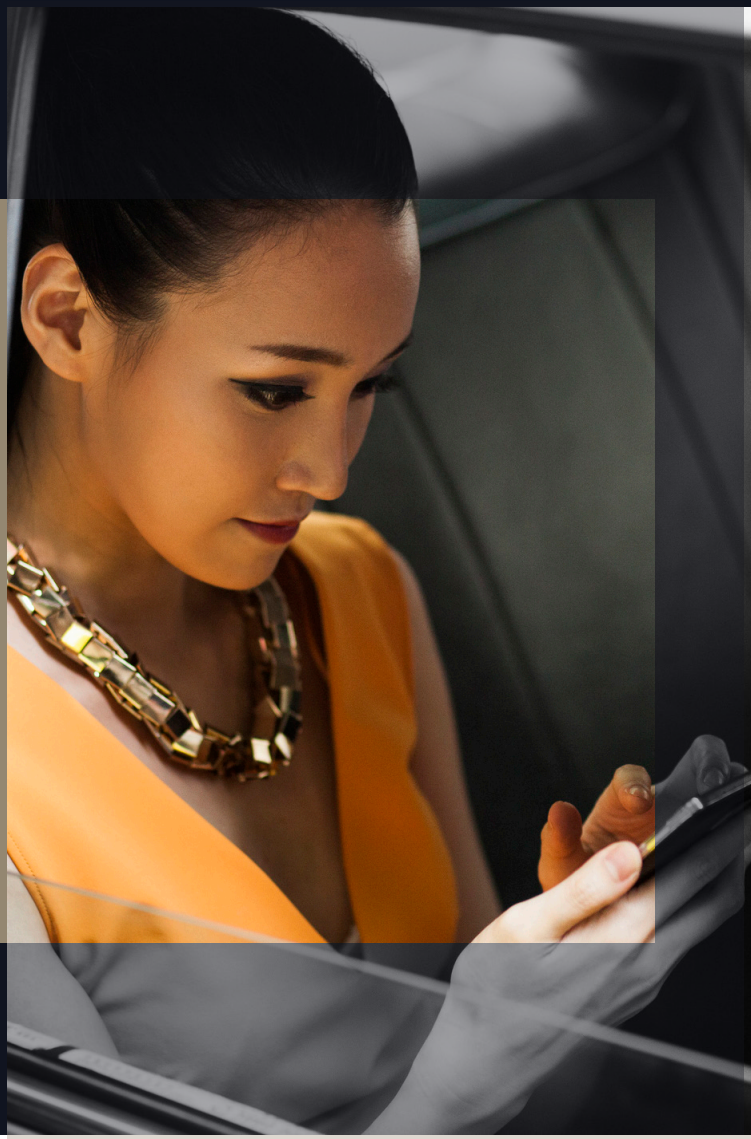
Check with your wireless provider:
Different wireless providers offer various tiers of SMS blocking capabilities. It's a good idea to contact your provider and understand what additional measures they can provide to help you safeguard against smishing.

Report spam messages:
Lastly, if you receive a spam message, you can forward it to 7726 (SPAM). When doing this, you send the information to your carrier and help them track and block future spam. Alternatively, if available, you can use your phone's built-in spam reporting features.

Where to look:

In addition to the tips on the previous page, if the following scenarios apply to an email you have received, it could indicate a smishing attack.

- I was cc'd on an email sent to one or more people, but I don't personally know the other people it was sent to.
- I received an email that was also sent to an unusual mix of people. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.



Get a Demo

Cyber threats like smishing are a reality of our digital age, but that doesn't mean we are helpless against them. By staying vigilant and practicing good cyber hygiene, we can significantly reduce the risk these threats pose to our privacy and security. At BlackCloak, we are committed to helping individuals navigate these complexities, providing expertise to maintain your cyber peace of mind.

Remember, your first line of defense against any cyber threat is you.

To learn more, please visit:

blackcloak.io