Vishing and Smishing Attacks

Vishing: a social engineering attack carried out via phone call or voicemail

Smishing: an attack that uses SMS or text messages

SOCIAL ENGINEERING ISN'T LIMITED TO EMAILS

Phishing scams are one of the most common social engineering attacks today. Scammers use emails, phone calls and texts to pose as company leadership, work colleagues, or clients to gain personal and confidential information about your company's people and business.

While the message may sound urgent, take caution when responding to any inquiries, whether it be via email, phone (call, text/SMS), or messenger (Microsoft Teams, Skype, WhatsApp, etc.).

HOW THESE SCAMS WORK

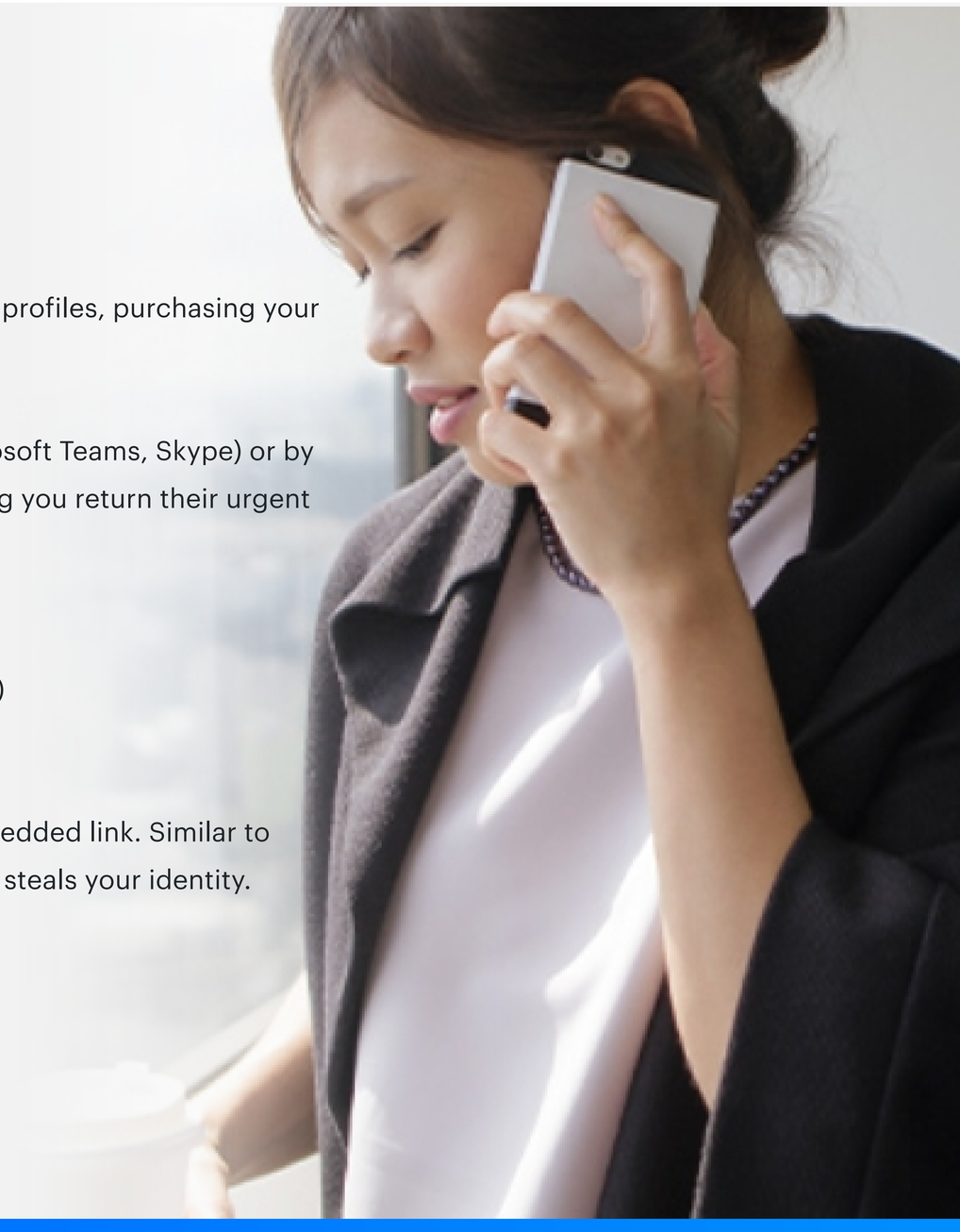
Scammers collect your credentials from a variety of sources; previous data breaches, social media profiles, purchasing your information on the dark web, or simply guessing correctly your contact information.

Armed with this data, scammers will reach out to you through an application (e.g. WhatsApp, Microsoft Teams, Skype) or by telephone (e.g. call, SMS/text) or email to solicit information. They may leave a voicemail requesting you return their urgent call. If you happen to engage with them, scammers may try to obtain:

- **Proprietary information** (client names, contract details, charge rates)
- **Individuals' personal information** (contact info, passwords, travel schedules, physical location)
- **Financial information** (accounting details, billing codes, credit card information)

For smishing attacks, scammers use a text or instant message, encouraging you to click on an embedded link. Similar to email phishing, clicking a link on your device can launch malware that captures your credentials or steals your identity.

For best practices, never click links, reply to text messages, or call numbers you don't recognize.



TYPICAL SMISHING SCAM EXAMPLES

Congratulations! You've won a $1,000 gift certificate from XYZ retailer. Click here to claim your prize: http://claim.mi.XYZprize

Your account has been deactivated. Click http://i.luva.scam to reactivate.

Your account has been locked. Click this link to unlock.

Your credit card has been locked due to unusual activity. Click here to unlock.

WHAT TO LOOK OUT FOR

Because scammers often spoof their IDs, it can be difficult to determine from caller ID alone that a call is legitimate.
Stay vigilant! Treat any unknown caller or text sender with caution.

Those seeking information for malicious reasons can be intimidating and convincing. They may reiterate their purported leadership status and appear knowledgeable by asking for employee or client team information by name.

If you receive a call from a number you do not recognize, keep the following in mind:

- ☑ **Do not provide any information**
- ☑ **Offer to take down the sender or caller's ID and contact phone number in order to verify the request**
- ☑ **End the dialogue stating you need to verify the caller's information**

If you receive a text from a number you do not recognize, keep the following in mind:

- ☑ **Never click links, reply to text messages, or call numbers you don't recognize**
- ☑ **Do not respond, even if the message requests that you "text STOP" to end messages**
- ☑ **Always review all texts from your bank / financial institution**
  Should you identify questionable charges/interactions contact your bank or financial institution immediately to determine if the text was legitimate or not
- ☑ **Delete all suspicious texts, blocking the numbers if possible**

We recognize many of you use WhatsApp personally and advise you to update as needed due to reported security vulnerabilities.

The only way to validate the legitimacy of an inquiry is to contact the source through another avenue or send another email to confirm the request.