



## INVESTIGATE

**EVIDENCE #1**

You have a new email!

FROM: National Police Force <[warning@nationalpolice-payment.com](mailto:warning@nationalpolice-payment.com)>

SUBJECT: Pay your outstanding fine or get arrested.

**NATIONAL POLICE FORCE****OFFICIAL**

This is your **final warning** to pay the outstanding fine you were charged two weeks ago.

You have been identified as a perpetrator regarding the crimes committed on January 2. We have CCTV evidence of you breaking the law.

We are charging you with a fine of \$2,000.00 in relation to this crime. Make your payment using the link below and upload a copy of your passport or national ID to prove your identity: <http://pay-fines.nationalpolice-payment.com/?123g73j>

If you do not pay this fine by **11:59 pm tonight**, we will escalate the charges to a felony crime and will come to your address to arrest you.

Ignoring this email is also considered a crime. If you do nothing, we will come and arrest you in 24 hours.

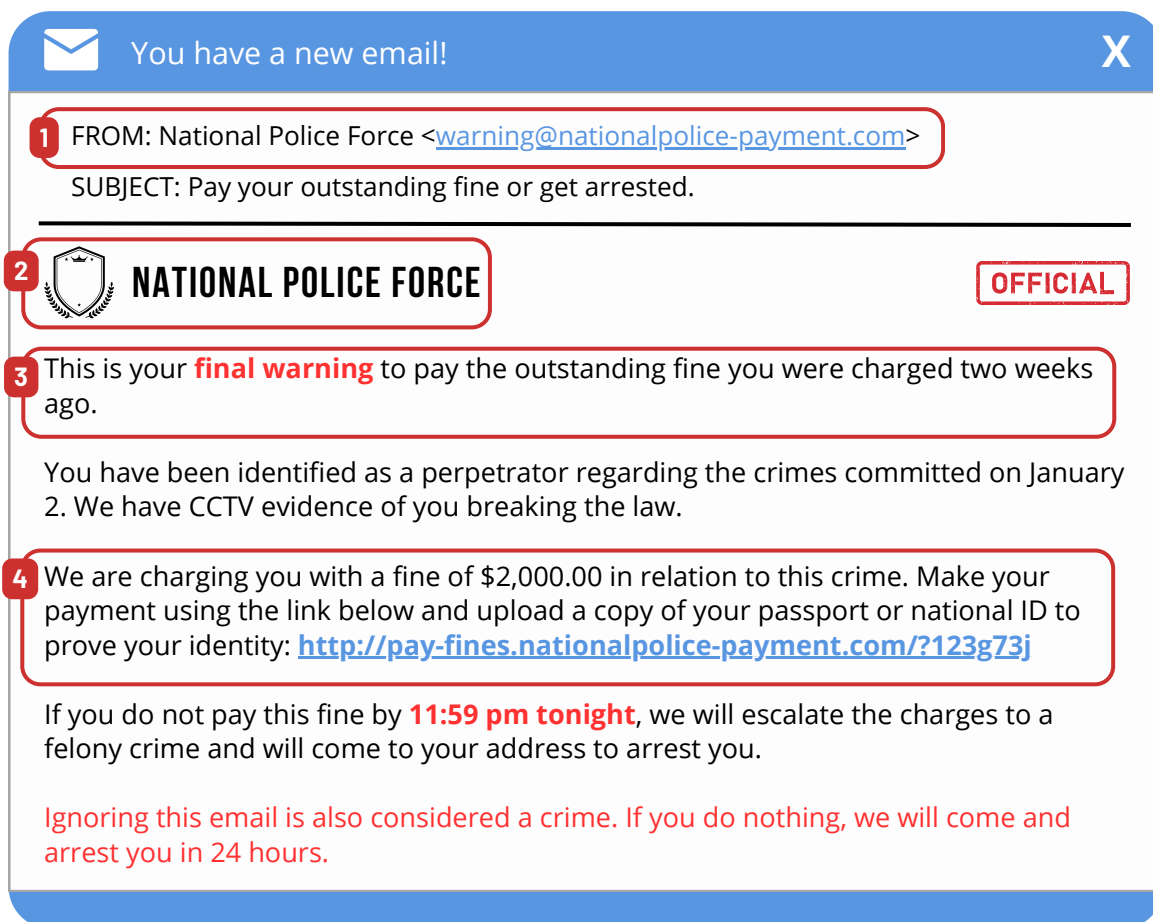
Which tactic(s) has the scammer used here?

1. Urgency
2. Intimidation
3. Love bombing

Identify all the clues that tell you this is a phishing scam.



## INVESTIGATE

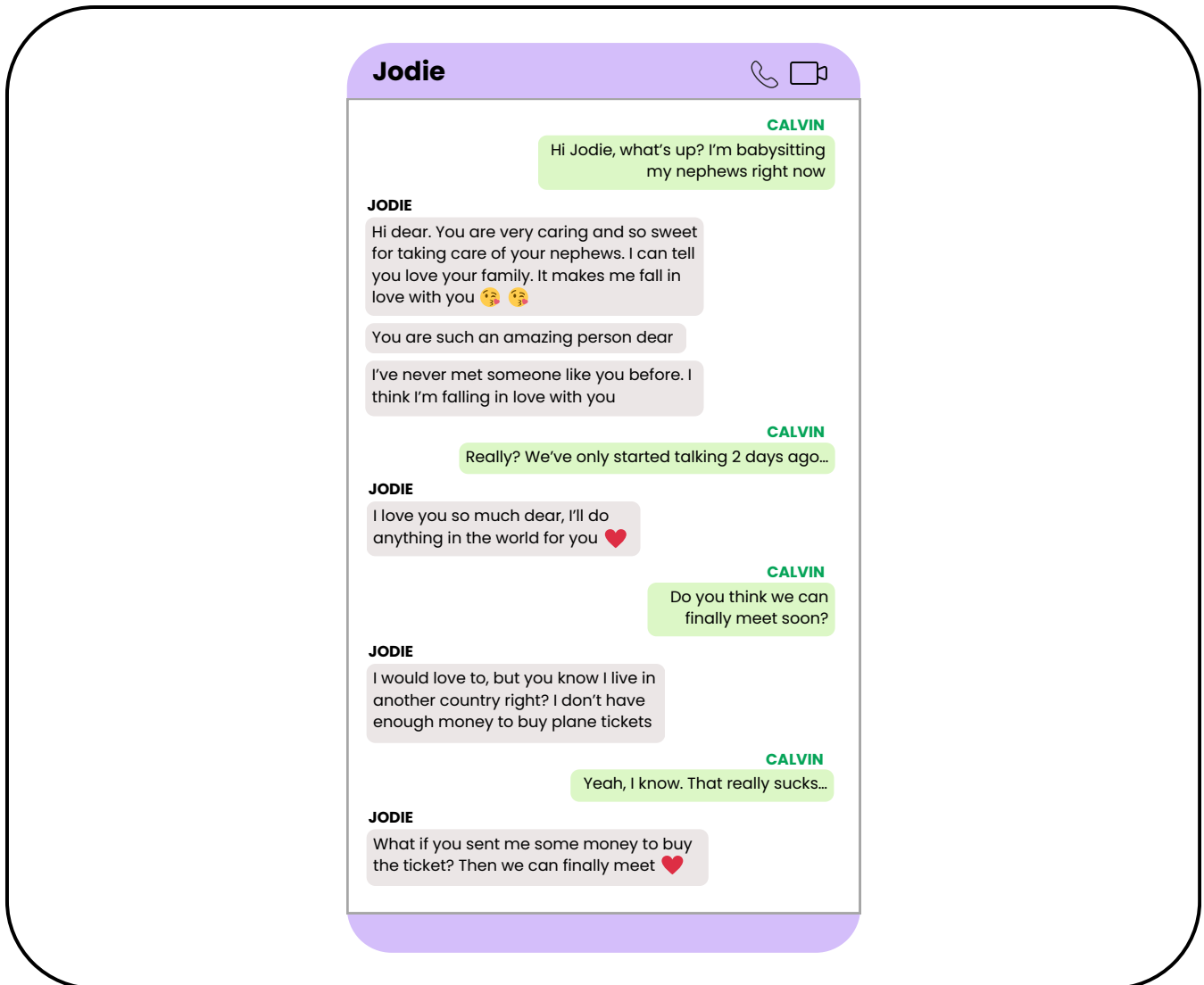
**EVIDENCE #1**

**WHAT?** Intimidation and urgency

**WHY?** To scam victims of money and personal information

### RED FLAGS TO LOOK OUT FOR:

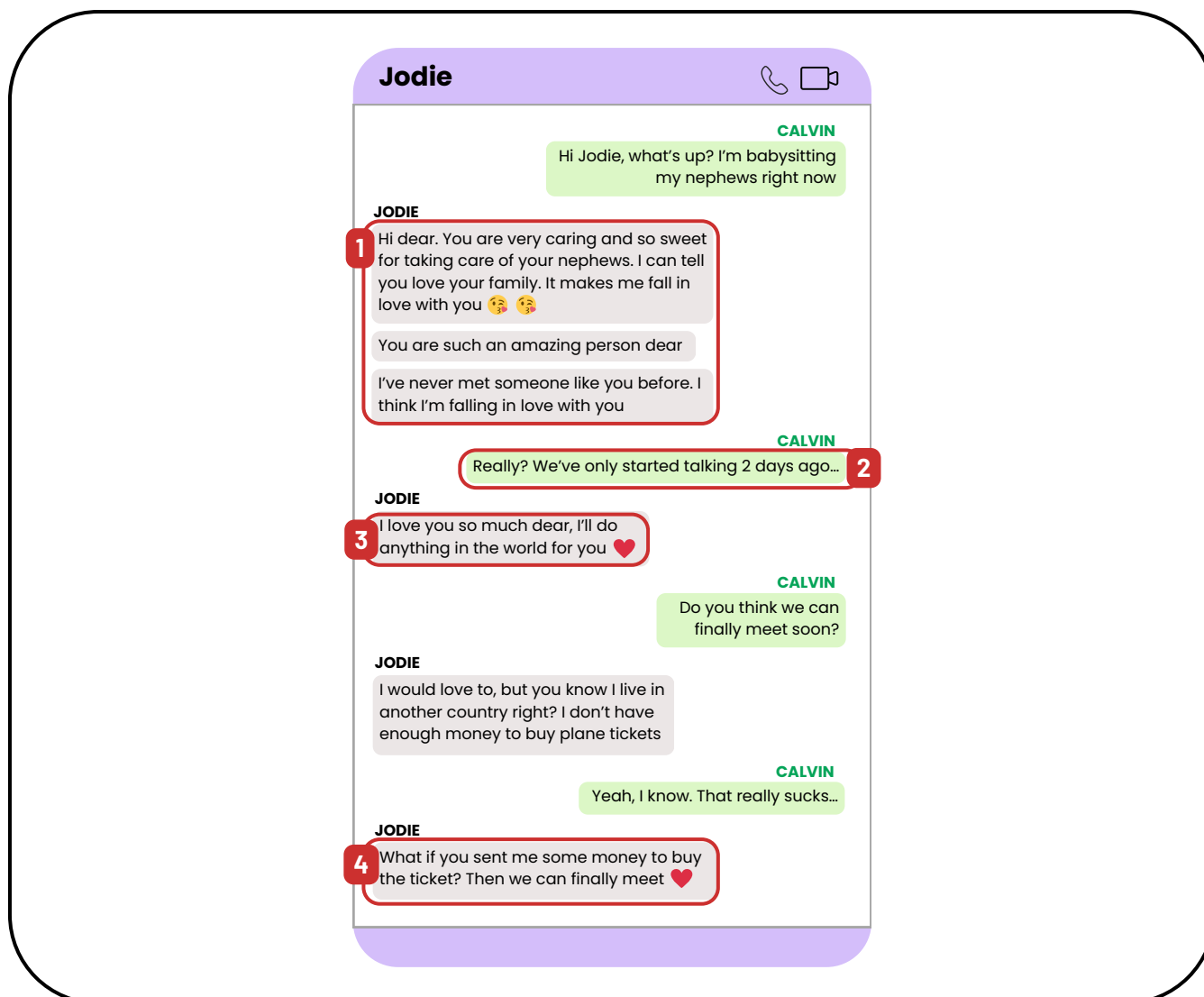
1. Always check the sender before acting out of fear. If you are unsure, call the official or national helpline to verify the email.
2. Scammers may use official logos to trick users. Don't blindly believe the message because of the logo.
3. The intimidating and urgent nature of the message can make you act carelessly. Seek help from trusted adults or official authorities.
4. Always check the URL before making payments or providing personal information.

**INVESTIGATE****EVIDENCE #2**

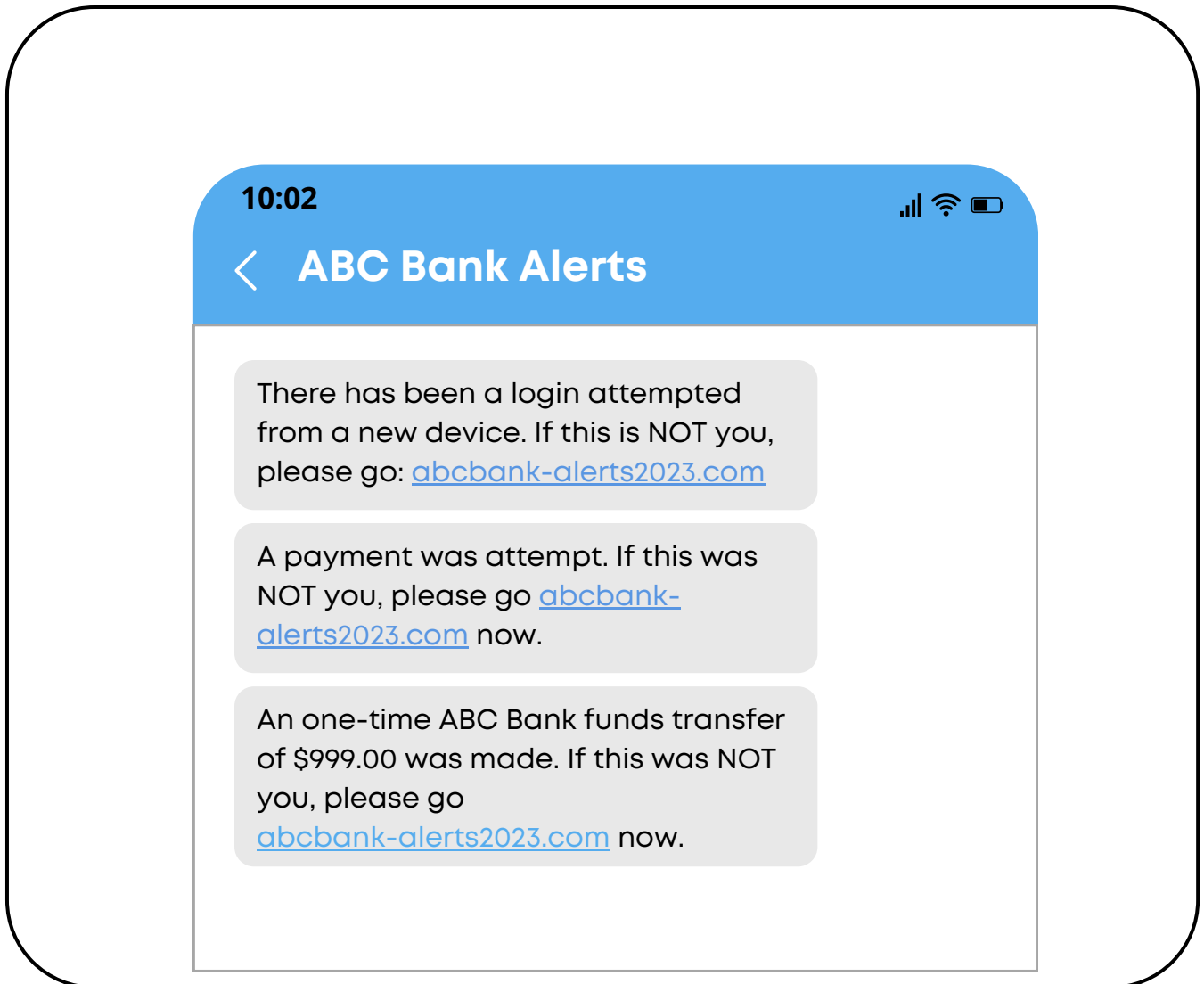
Which tactic(s) has the scammer used here?

1. Urgency
2. Intimidation
3. Love bombing

Identify all the clues that tell you this is a phishing scam.

**INVESTIGATE****EVIDENCE #2****WHAT? Love bombing****WHY? To get victims to transfer money through romance scams****RED FLAGS TO LOOK OUT FOR:**

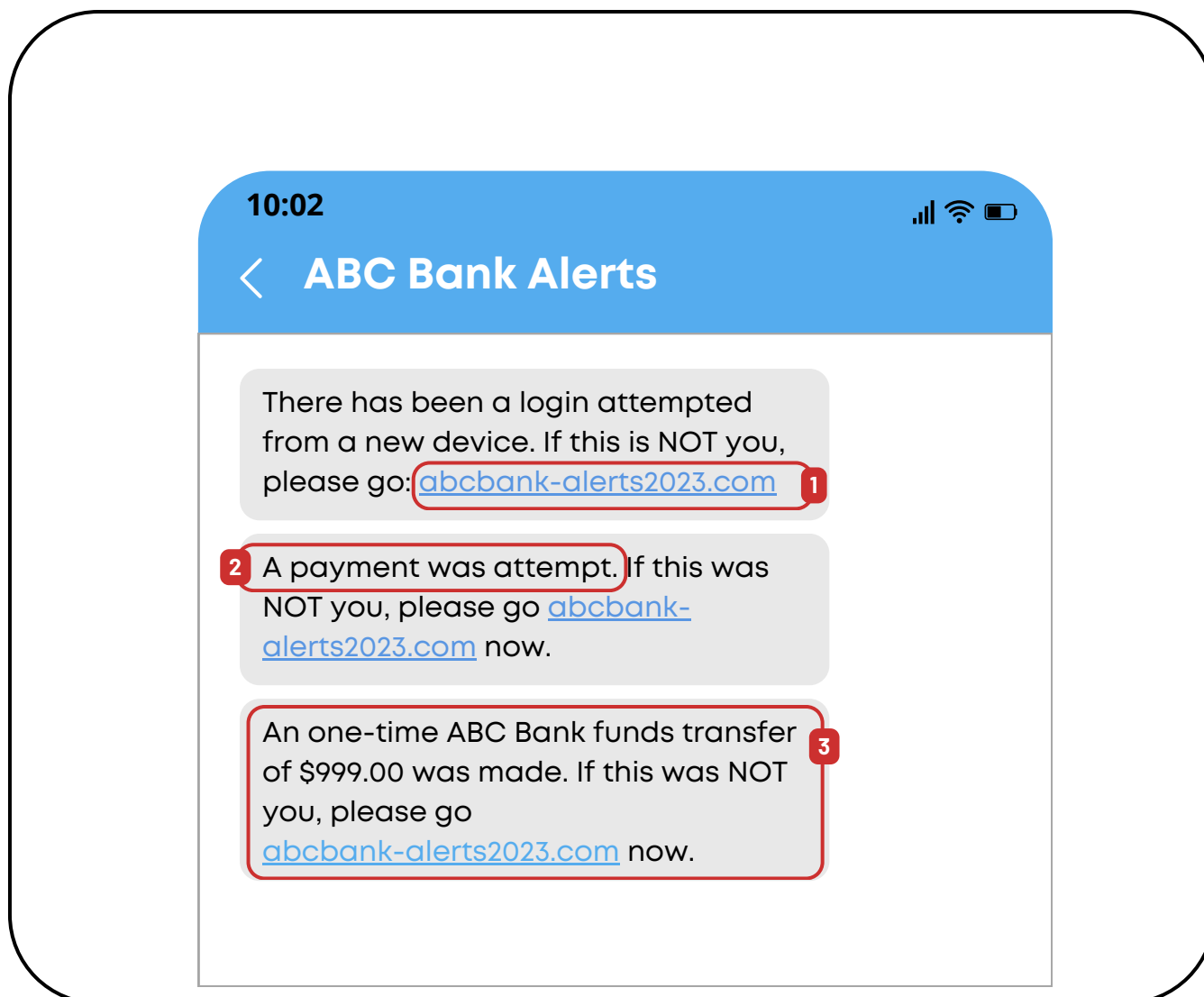
1. Love scammers will often shower you with flattery and compliments to gain your trust.
2. Love bombing can often feel like the relationship is moving very fast. Listen to your gut feeling to see if the pace feels unnatural or forced.
3. Jodie doesn't use a lot of personalised language (such as calling Calvin by name) and often mirrors what Calvin has just said without providing much information about herself.
4. Be careful of sending money to someone you don't know in real life.

**INVESTIGATE****EVIDENCE #3**

Which tactic(s) has the scammer used here?

1. Urgency
2. Intimidation
3. Love bombing

Identify all the clues that tell you this is a phishing scam.

**INVESTIGATE****EVIDENCE #3****WHAT? Urgency****WHY?** To steal login credentials, banking details, or personal information through phishing links**RED FLAGS TO LOOK OUT FOR:**

1. Always check the URL link before clicking to ensure it's the official address.
2. The grammatical errors in these messages are red flags. Official communications from banks will be written properly.
3. If you are unsure of a message's authenticity, call your bank's official hotline for assistance. Do not call any phone numbers that may be in the suspicious messages.



## PROJECT WORK

**Design a mock phishing attack using the tactics of urgency, intimidation, or love bombing. Demonstrate who your attack is targeted at, and how your phishing attack exploits the vulnerabilities in your targets.**

### **What should your project outcome look like?**

Your phishing attack can be delivered as an email, SMS, website, or on social media, and must include at least three elements that are designed to trick your target.

### **Instructions and Questions to Consider:**

1. Identify the target audience for your mock phishing attack. Who are they and what are their vulnerabilities that make them susceptible to falling for the scam?
2. Decide on the tactics that you will use to exploit your target's vulnerabilities. Will you use urgency, intimidation, or love bombing tactics, or a combination of these?
3. Choose the delivery method for your attack. Will you send an email, SMS, create a fake website or use social media to deliver your attack?
4. Create at least three elements in your attack that are designed to trick your target.
5. Write a reflection on what you learned about the tactics used in phishing attacks and how to protect yourself from them.