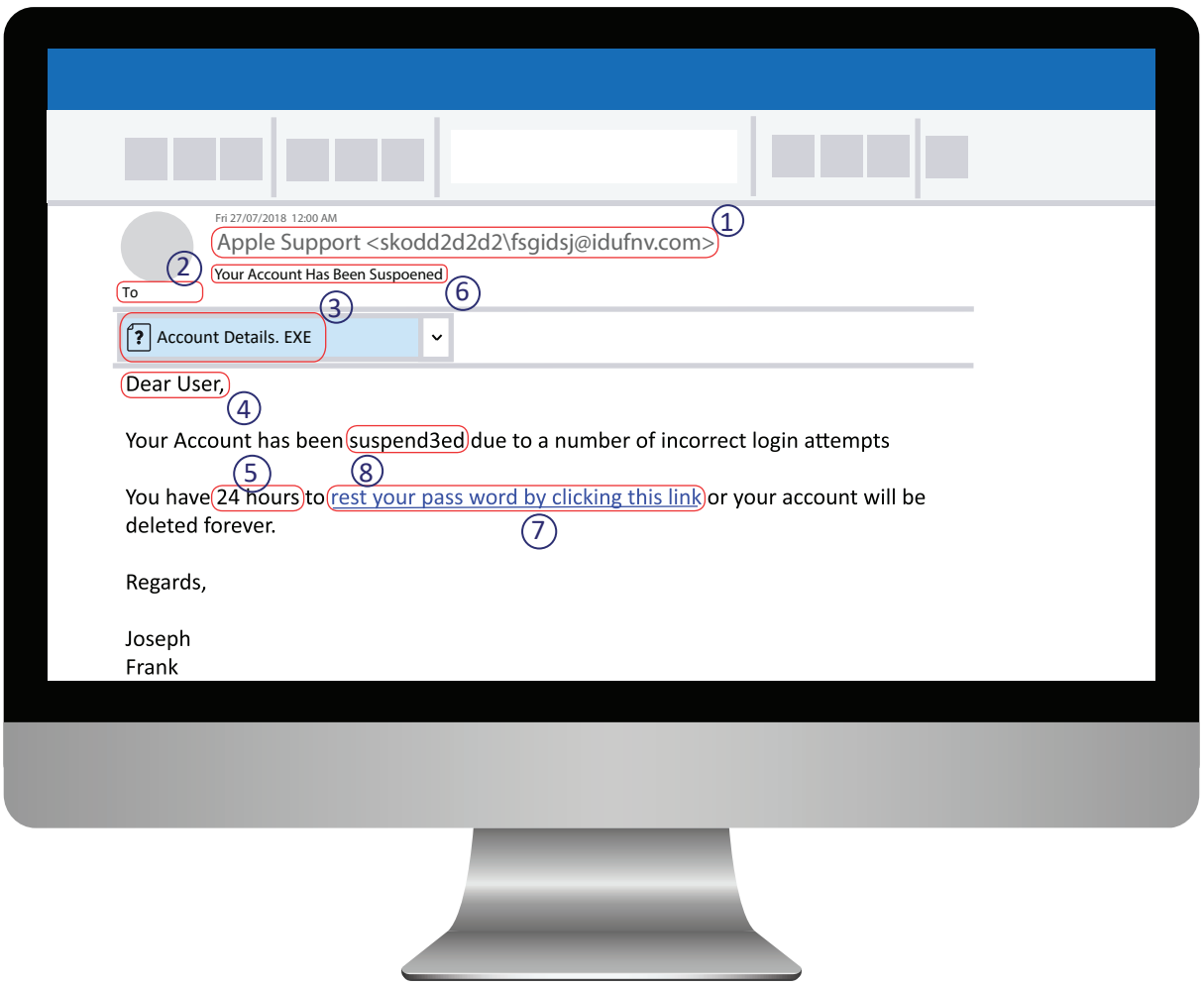
How to identify a fake email

Microsoft Outlook



8-point checklist:

1. **Sender.** This is the first thing to check. If the email address doesn't match the displayed company name (such as like this: eBay support@youraccount.xyz) do not click on any links. The sender is trying to trick you with a fake name.

2. **'To' field.** If the field is blank, then you have been BCC'd (Blind CC'd). This can be done for legitimate reasons, but is very uncommon, and virtually non-existent if you do not know the sender.

3. **Attachments.** It is never safe to open attachments from email addresses you don't know, no matter the type of file. In addition, even known email addresses can send you infected files, whether unintentionally or due to the sender being infected. Just remember, if in doubt, don't download or open any files.

4. **How you're addressed.** According to PayPal, 'Impersonal, generic greetings are used. Greetings such as "Dear user" or "Dear [your email address]" are easy detectors. Most reputable companies will only ever use your first name.

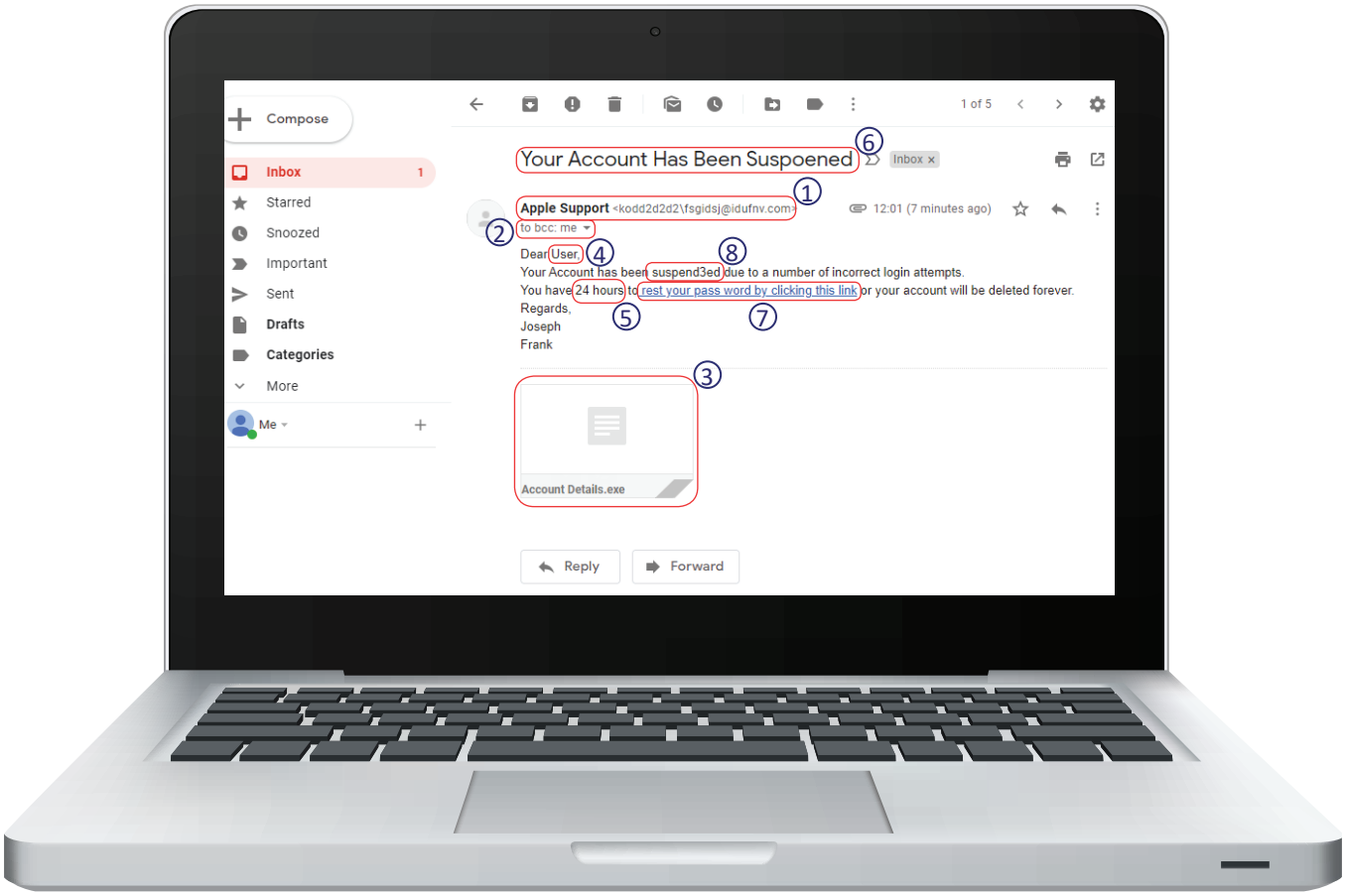
5. **An actionable time frame.** This method is used to scare people into acting quickly without thinking. This way, people are more often going to give up their account details without thinking.

6. **"Your Account has been suspended", "Reset Password", etc.** Large companies (eBay, PayPal, Facebook, etc.) do not send emails like this asking for account details. Don't ever click on the links and, if you do, never enter any information, it will go straight to hackers.

7. **Embedded hyperlinks.** These are a great way to cover up which website you are going to. You might be thinking that you're going to Facebook.com, but in reality, you're being taken to hackersyourpassoword.com.au.

8. **Spelling mistakes.** Most of these hackers are from foreign countries where English is not their first language. The large companies that they pretend to be have professional Copywriters who don't make spelling mistakes

netway networks



How to identify a fake email

Gmail

8-point checklist:

1. **Sender.** This is the first thing to check. If the email address doesn't match the displayed company name (such as like this: eBay support@youraccount.xyz) do not click on any links. The sender is trying to trick you with a fake name.

2. **'To' field.** If the field is blank, then you have been BCC'd (Blind CC'd). This can be done for legitimate reasons, but is very uncommon, and virtually non-existent if you do not know the sender.

3. **Attachments.** It is never safe to open attachments from email addresses you don't know, no matter the type of file. In addition, even known email addresses can send you infected files, whether unintentionally or due to the sender being infected. Just remember, if in doubt, don't download or open any files.

4. **How you're addressed.** According to PayPal, 'Impersonal, generic greetings are used. Greetings such as "Dear user" or "Dear [your email address]" are easy detectors. Most reputable companies will only ever use your first name.

5. **An actionable time frame.** This method is used to scare people into acting quickly without thinking. This way, people are more often going to give up their account details without thinking.

6. **"Your Account has been suspended", "Reset Password", etc.** Large companies (eBay, PayPal, Facebook, etc.) do not send emails like this asking for account details. Don't ever click on the links and, if you do, never enter any information, it will go straight to hackers.

7. **Embedded hyperlinks.** These are a great way to cover up which website you are going to. You might be thinking that you're going to Facebook.com, but in reality, you're being taken to hackersyourpassoword.com.au.

8. **Spelling mistakes.** Most of these hackers are from foreign countries where English is not their first language. The large companies that they pretend to be have professional Copywriters who don't make spelling mistakes

netway networks