Project-1:Phishing Email Detection Guide

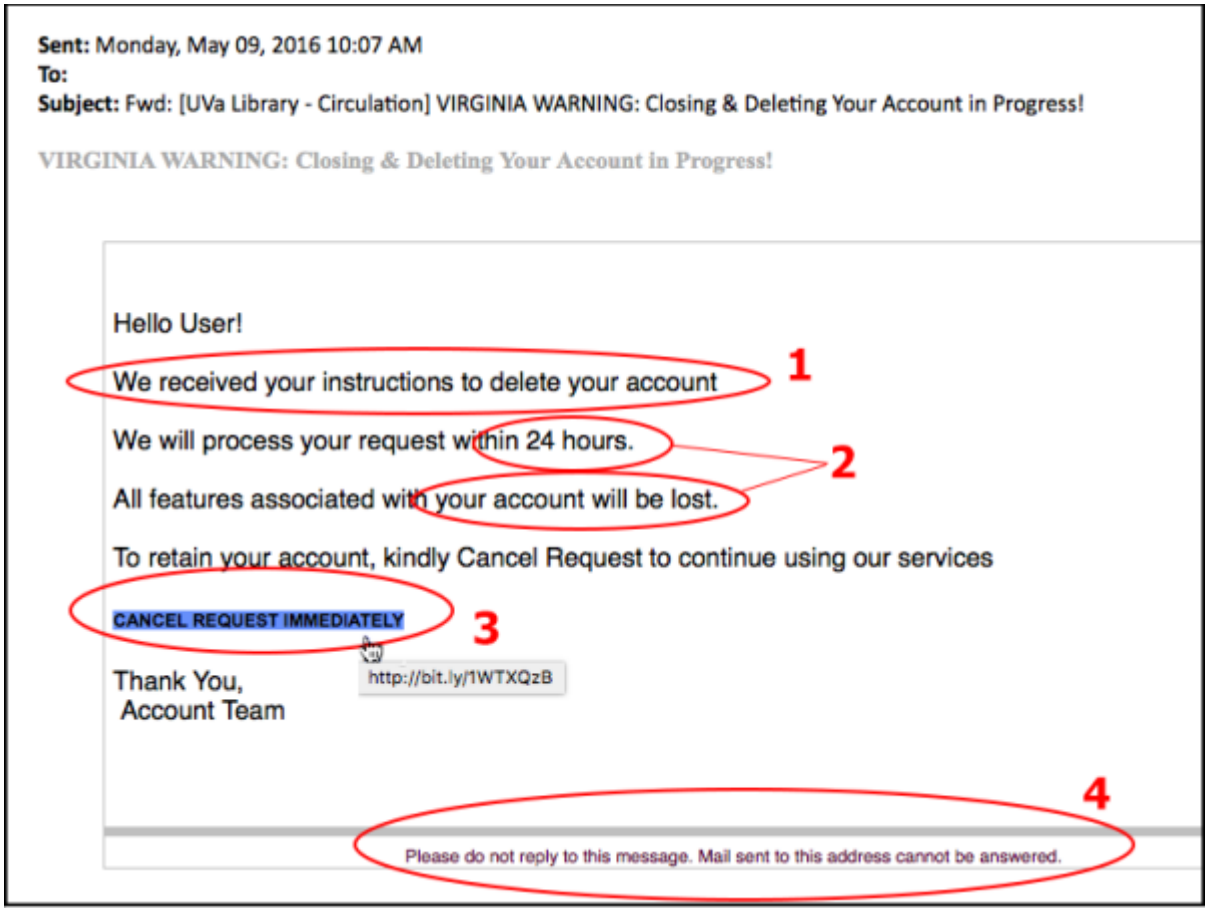
Phishing emails are fraudulent messages designed to trick users into revealing sensitive information such as passwords, bank details, or personal data. This guide highlights **common red flags** in phishing emails using real-world examples.

Example 1: Fake Account Deletion Notice

Red Flags:

1. Urgency – *"We received your instructions to delete your account"* creates panic.
2. Time pressure – *"within 24 hours"* forces quick action.
3. Suspicious button – *"CANCEL REQUEST IMMEDIATELY"* links to a shortened/unknown URL.
4. No reply option – discourages contacting legitimate support.

Tip: Always verify such claims directly from the official website instead of clicking links in the email.

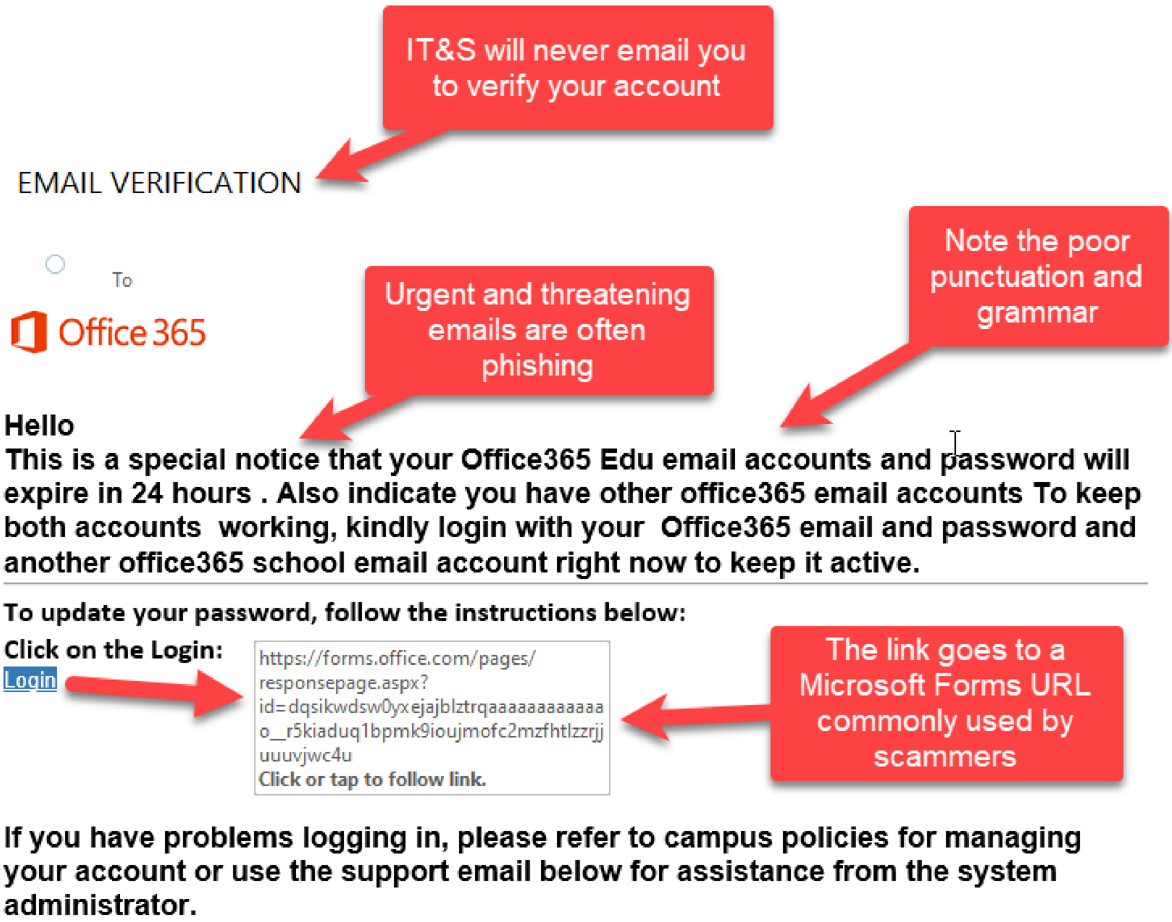


Example 2: Fake Office 365 Verification

Red Flags:

- Poor grammar & punctuation.
- Urgent language – *“expire in 24 hours”*.
- Link disguised as Microsoft but actually goes to a **fake Microsoft Forms page**.
- IT departments never ask you to verify accounts this way.

Tip: Hover over links to check their true destination.



Example 3: Fake Rackspace Alert

Red Flags:

- Suspicious sender email – not from official Rackspace domain.
- Fake security concern – *“multiple login attempts”*.
- Malicious link disguised as Rackspace login but actually redirects elsewhere.

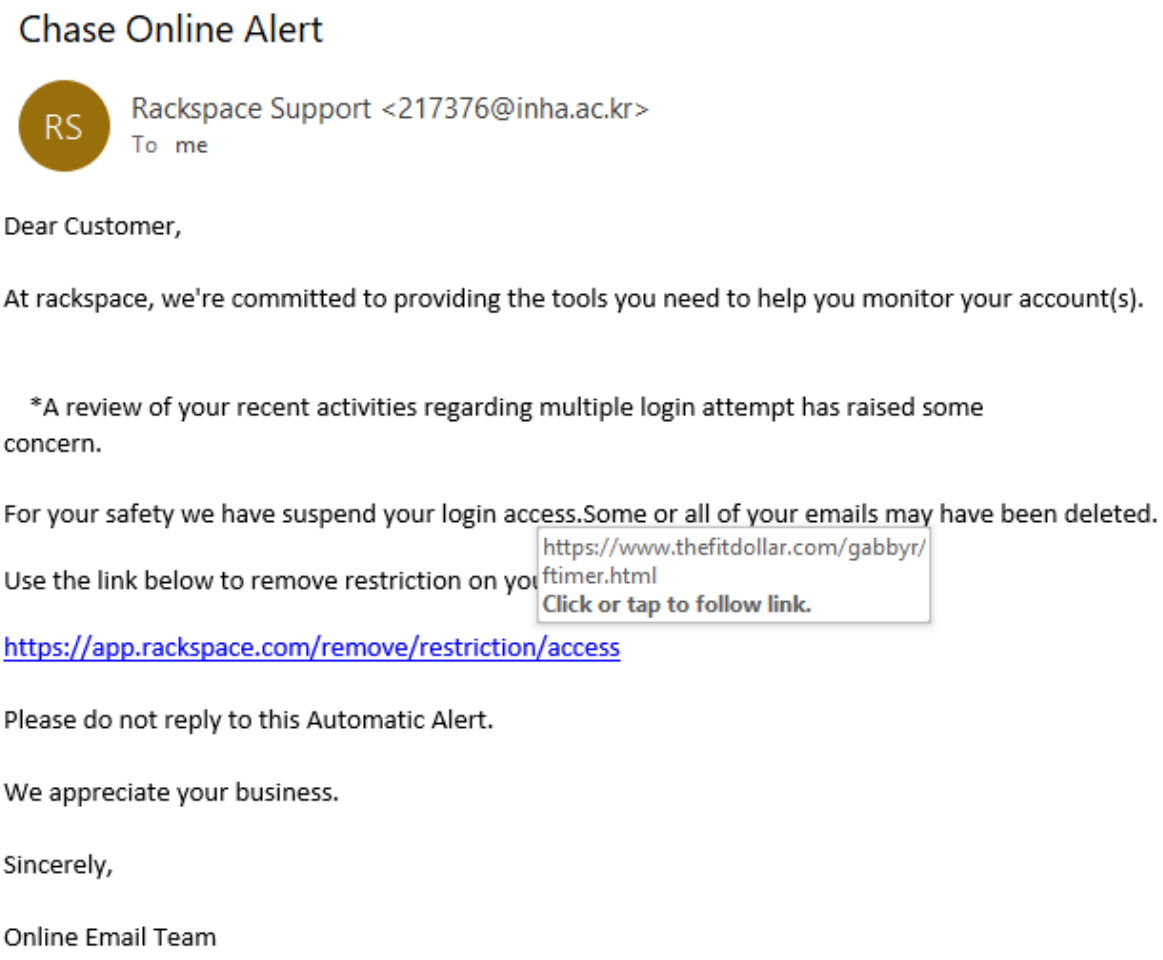
Tip: If you suspect login issues, visit the service provider’s official website manually.

Example 3: Fake Rackspace Alert

Red Flags:

- Suspicious sender email – not from official Rackspace domain.
- Fake security concern – *"multiple login attempts"*.
- Malicious link disguised as Rackspace login but actually redirects elsewhere.

Tip: If you suspect login issues, visit the service provider's official website manually.



Chase Online Alert

RS Rackspace Support <217376@inha.ac.kr>
To me

Dear Customer,

At rackspace, we're committed to providing the tools you need to help you monitor your account(s).

*A review of your recent activities regarding multiple login attempt has raised some concern.

For your safety we have suspend your login access.Some or all of your emails may have been deleted.

Use the link below to remove restriction on yo

https://www.thefitdollar.com/gabbyr/ftimer.html
Click or tap to follow link.

https://app.rackspace.com/remove/restriction/access

Please do not reply to this Automatic Alert.

We appreciate your business.

Sincerely,

Online Email Team

Example 4: Fake Amazon Suspension

Red Flags:

- 👤 Generic greeting – *"Dear Client"* instead of your real name.
- 📧 Sender email is misspelled (`mazoncanada.ca` instead of `amazon.ca`).
- 🔗 Link claims to be Amazon but redirects to a non-Amazon site.

✅ **Tip:** Check the sender's domain carefully. Legit companies use official domains.

Example 4: Fake Amazon Suspension

Red Flags:

- Generic greeting – *"Dear Client"* instead of your real name.
- Sender email is misspelled (`mazoncanada.ca` instead of `amazon.ca`).
- Link claims to be Amazon but redirects to a non-Amazon site.

Tip: Check the sender's domain carefully. Legit companies use official domains.

How to Protect Yourself

- **Check sender email** – Is it from the official domain?
- **Beware urgency** – Phishing often pressures you to act fast.
- **Hover over links** – Don't click unless you're sure.
- **Never share credentials** through email links.
- **Report phishing emails** to your email provider or IT team.

Portfolio Note:
This project demonstrates my ability to **analyze phishing emails**, highlight security red flags, and create **educational cybersecurity awareness material**.