ICT DEPARTMENT

PHISHING 101

Think before you click!

PRE-TRAINING TEST

PHISHING 101

Think Before You Click

Take the pre-training test

WHAIT IS PHISHING ?

“**Phishing is** an online scam where criminals send fraudulent email messages, appearing legitimate. The emails contain links or attachments that trick recipients into entering confidential information (e.g. account numbers, passwords) into fake websites, or they infect computers with malware.”

"Think back to a time you got an email or message asking for your private data. What were the red flags that made you think twice?"

SOUND FAMILIAR ?

You're busy at work, and an email suddenly pops up saying

1

Your account has been suspended

2

Please confirm your invoice to avoid service interruption

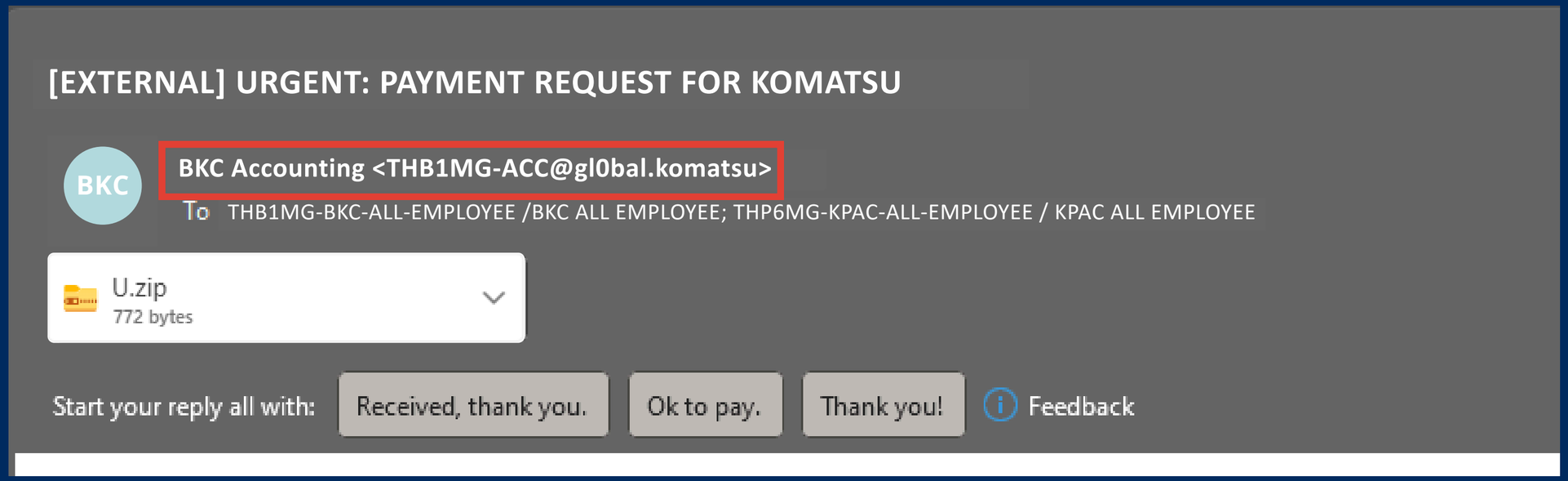
3

Congratulations, you've won a grand prize!

These emails might look like they're from a trusted company, your bank, or even a government agency.
But in reality... it could be a trap!

5 RED FLAGS TO SPOT PHISHING EMAILS

1. "WHO SENT IT?" - CAREFULLY CHECK THE 'DOMAIN'



Scammers often use 'domains that look similar to the real one'. For example, an email from THB1MG-ACC@gl0bal.komatsu uses the number 0 instead of the letter O ❌

The real domain for our company is @global.komatsu ✅

2."WHAT'S THE RUSH?" - THE SUBJECT AND CONTENT CREATE A SENSE OF URGENCY AND PRESSURE

1 [EXTERNAL] 【IMPORTANT】 Login Re-authentication Required Due to Internal Portal Maintenance 2

SystemSupport<support@intra-portal.jp>
To: Teachasit Seeha

Hello!
This is a notification from the Internal Portal Management Team, IntraPortal Support.

3 We are currently conducting scheduled maintenance on the internal portal system.
After the maintenance is completed, all users are required to re-authenticate their login credentials to enhance security.

Please access the following link and enter your login information (ID and password) to complete the re-authentication process:

▼Re-authentication Page
https://intra-portal.jp/auth-update

Please note:
・If re-authentication is not completed, access to the portal may be restricted.
・Please complete this process by the end of today.

If you have any questions, feel free to contact IntraPortal Support.

Best regards,

IntraPortal Support
Internal Portal Management Team

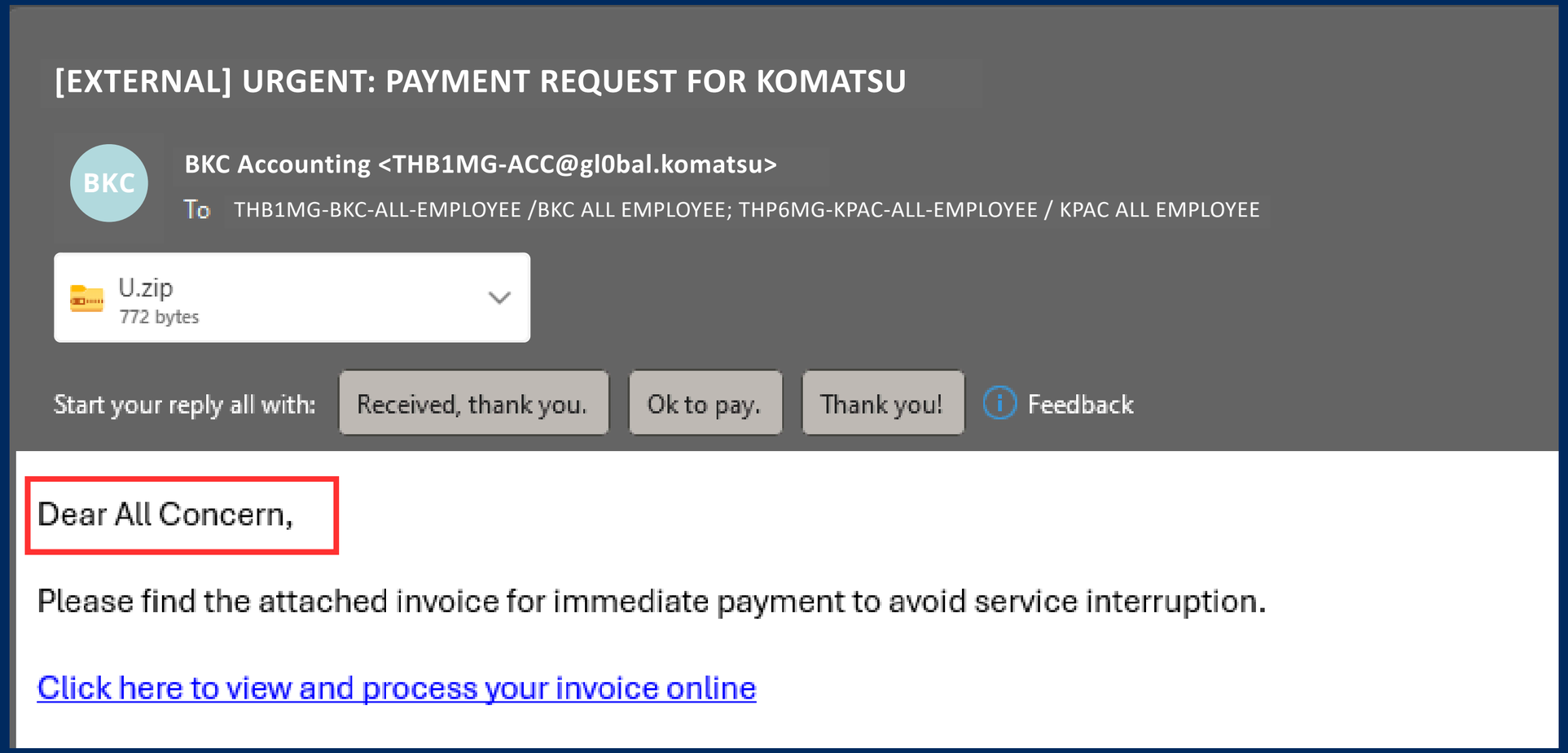
1.[EXTERNAL] → THIS EMAIL IS FROM AN EXTERNAL SENDER

2.URGENT → CREATES A SENSE OF PRESSURE

3.THREATS → USES FEAR TACTICS LIKE, "THERE WILL BE NEGATIVE CONSEQUENCES," OR "YOUR SERVICE WILL BE CUT OFF

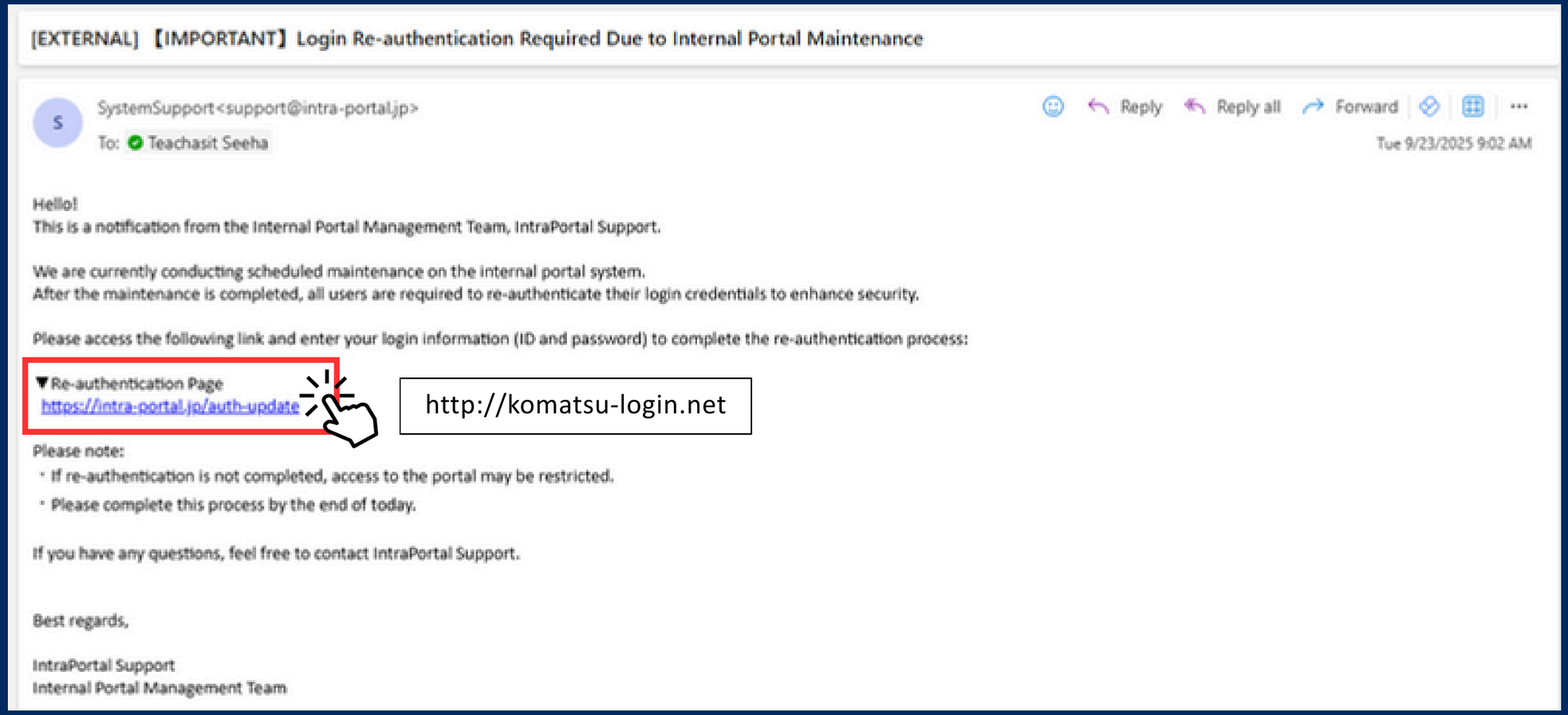
If an email has all three of these components “External sender + Urgency + Threats” it is highly likely to be a phishing emai

3. "GENERIC GREETING" - THE SALUTATION DOES NOT SPECIFY YOUR NAME.



Emails from legitimate organizations usually include your first and last name. However, phishing emails often use broad greetings like 'Dear Employee' or 'Dear All'

4. "SUSPICIOUS LINKS" - CHECK THE LINK BEFORE YOU CLICK



[EXTERNAL] 【IMPORTANT】Login Re-authentication Required Due to Internal Portal Maintenance

S SystemSupport<support@intra-portal.jp>

To: Teachasit Seeha

Reply Reply all Forward

Tue 9/23/2025 9:02 AM

Hello!
This is a notification from the Internal Portal Management Team, IntraPortal Support.

We are currently conducting scheduled maintenance on the internal portal system.
After the maintenance is completed, all users are required to re-authenticate their login credentials to enhance security.

Please access the following link and enter your login information (ID and password) to complete the re-authentication process:

▼Re-authentication Page
https://intra-portal.jp/auth-update

http://komatsu-login.net

Please note:
・If re-authentication is not completed, access to the portal may be restricted.
・Please complete this process by the end of today.

If you have any questions, feel free to contact IntraPortal Support.

Best regards,

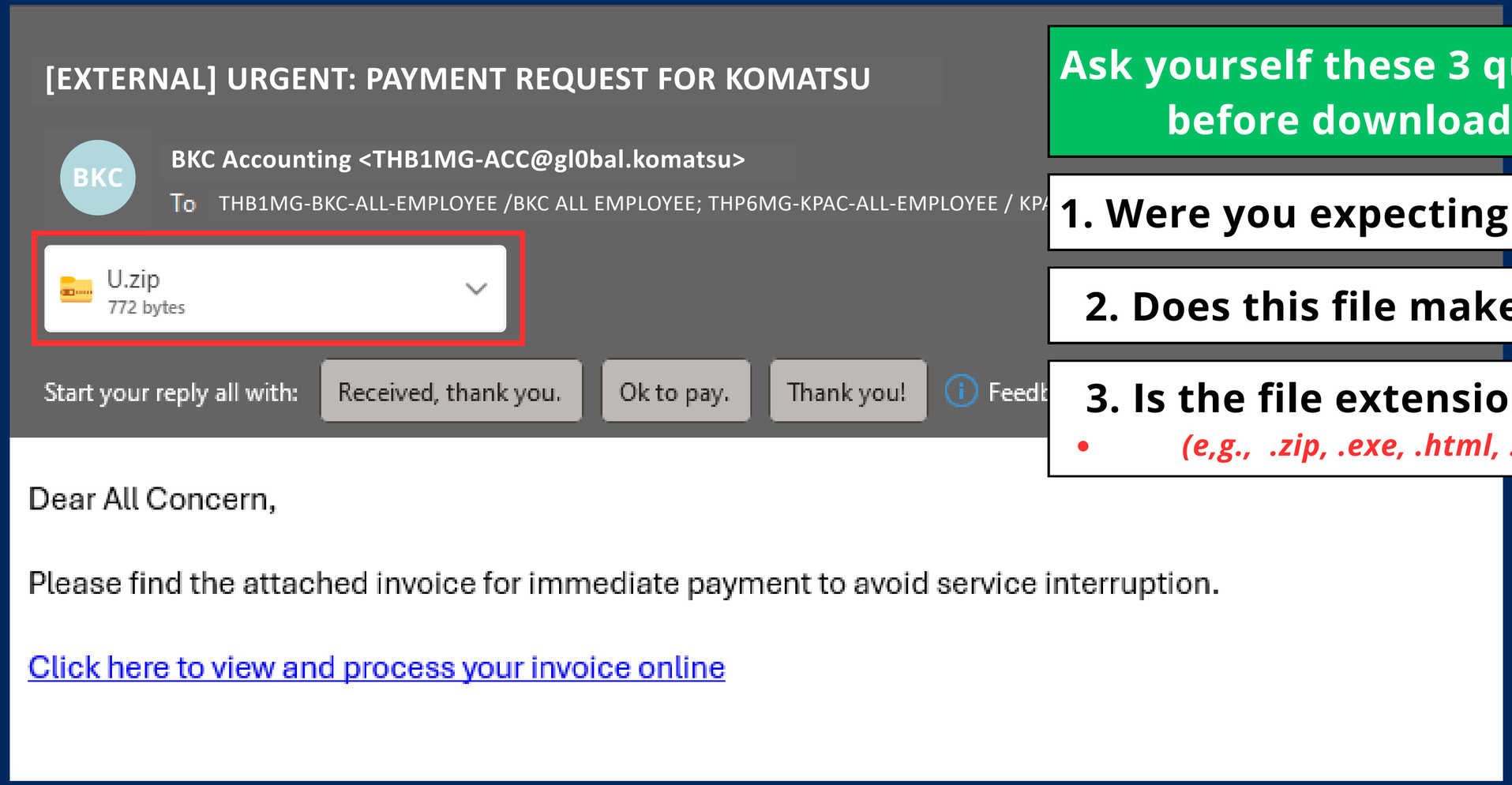
IntraPortal Support
Internal Portal Management Team

1.Hover → Hover your mouse over the link.

2.Look → Read the URL that appears.

3.Think → "The destination is http://komatsu-login.net" ❌.
The company's correct website domain is .bkc.co.th or or a trusted vendor's official domain ✅.

5. "DANGEROUS ATTACHMENTS" - DO NOT RUSH TO DOWNLOAD



Ask yourself these 3 questions before downloading:

1. **Were you expecting this file?**
2. **Does this file make sense?**
3. **Is the file extension risky?**
   - *(e,g., .zip, .exe, .html, .js, .scr)*

Unsure? → Call the sender directly! (Do not reply to the email).

WHAT TO DO
IF YOU ENCOUNTER PHISHING?

01 **DON'T:** 🚫 - Do not click any links in the email.

02 **DON'T:** 🚫 - Replying confirms your email address is active.

03 **DON'T:** 🚫- Open Attachments!

04 **DO:** Notify the IT Department! 📧 - Forward the suspicious email to the IT Department immediately for review.

05 **DO:** 🗑️ After reporting it to the IT Department, delete the email from your inbox.

THINK BEFORE YOU CLICK!

5 Red Flags to Check

- Sender?
- Urgent content?
- Generic greeting?
- Suspicious link?
- Suspicious attachment?

Use this Technique

- Hover over the link.
- Look at the URL that appears.
- Think before you click.

Unsure? Report ICT!

- Don't click! 🛑
- Don't reply! 🛑
- Report it immediately!

SMISHING & VISHING

- New forms of cyber threats often rely on urgency and impersonation as their main tactics.
- Leaked information (such as OTPs, ID cards, or bank accounts) poses risks to both the company and individuals.
- Serious damage can begin with just one click or one reply.

WHAT IS SMISHING (SMS + PHISHING)

- Short text messages with fake links, e.g., parcel notifications, payment alerts
- Designed to **lure users** into entering personal data or downloading malware
- Warning signs: **urgent tone, spelling errors, unusual domain names**

WHAT IS VISHING (VOICE + PHISHING)

- Phone scams pretending to be from banks, government offices, or HR
- Attackers ask for confidential info (account numbers, OTPs, or money transfers)
- Some even use AI-generated voices to sound like legitimate callers

DO

✅ Verify first: **Use official apps, websites, or verified phone numbers**

✅ Report immediately: **Take a screenshot and inform the ICT team**

✅ Keep your **devices** and apps updated with anti-malware enabled

DON’T

❌ Don’t **click links** from unknown or suspicious SMS

❌ Don’t **share passwords, OTPs, or financial details** by phone

❌ Don’t **call back** numbers in suspicious messages

THINK BEFORE YOU CLICK!

PROTECT YOURSELF FROM PHISHING

Don't share your personal information online!

POST-TRAINING TEST

Take the post-training test

Think Before You Click