Email Security Guideline (Staff)

Organization: Tree (tree.com.hk)
Prepared by: Max.chan@mediaworld.com.hk
Approved by:
Date: 2026-01-15
Version: ESG-v1.0

For: All office users (tree.com.hk)
Related policy: System User Access Management · Computer Operations

Golden rules

1. **Do not open dirty / suspicious links**
2. **Do not open unexpected attachments**
3. **Do not share your password** with anyone
4. **Verify the sender address** — especially for unusual requests
5. If unsure → **stop** and ask **Admin**

Email sender verification

Always check the **real From address** (not only the display name). Display names can be faked.

When to double-confirm

If the email asks for something **unusual** or unexpected, **stop** and double-confirm the sender before acting, for example:

- Urgent payment, bank transfer, or Visa / card details
- Password, OTP, or account login request
- Change of bank account / supplier details
- Request to buy gift cards, or send money “right now”
- Unusual instruction from a boss / manager / colleague you were not expecting

How to confirm: check the full email address carefully, then confirm by another channel (phone / in person / known chat) — do **not** use a reply, phone number, or link inside the same suspicious email.

Watch for misspelled email addresses

Attackers often use addresses that look almost right. Check every character:

Look for	Example of fake	Real
Wrong domain	`name@tree.com` or `name@tre.com.hk`	`@tree.com.hk`
Extra / missing letter	`name@tree.com.hk` (look-alike letter)	`@tree.com.hk`
Extra word / hyphen	`name@tree-hk.com` / `name@secure-tree.com.hk`	`@tree.com.hk`
Wrong person	Display name “Boss” but address is unknown	Known colleague `@tree.com.hk`

- Open / expand the sender details and read the **full address**
- Compare it to an address you already trust (previous real email, company directory)
- Any misspelling or almost-correct address → treat as **suspicious** and report to **Admin**

What is a “dirty” / suspicious email?

Be careful if the email:

- ☐ Comes from an unknown sender
- ☐ Looks like a known company or colleague but the address is slightly wrong / misspelled
- ☐ Makes an unusual request (money, password, urgent action) without prior notice
- ☐ Has urgent / scary language (“account locked”, “pay now”, “click now”)
- ☐ Has a strange link or shortened URL
- ☐ Has an unexpected file (`.exe` , `.zip` , `.js` , or unknown type)
- ☐ Asks for password, bank, or Visa card details
- ☐ Has poor spelling / odd greeting

Do

- [ ] Check the real sender address before clicking or acting on anything
- [ ] For unusual requests — double-confirm the sender is from the **correct** email address (watch for misspellings)
- [ ] Confirm unusual requests via another channel (phone / in person) — not by replying to the email
- [ ] Hover over links (do not click) to see where they go
- [ ] Use official websites / apps you already know — not links from email
- [ ] Report suspicious email to **Admin**
- [ ] Lock your PC when you leave your desk
- [ ] Keep your password private

Do not

- [ ] Click unknown or unexpected links
- [ ] Download / open dirty or unexpected attachments
- [ ] Reply with password, OTP, or card / bank info
- [ ] Act on unusual money / access requests without verifying the sender address
- [ ] Trust the display name alone (always check the full email address)
- [ ] Forward suspicious mail to many colleagues (report to Admin instead)
- [ ] Disable security warnings

Reminder — Tree systems

- Visa card payment info is handled by the **payment gateway** — Tree systems do **not** store card details
- Nobody from IT / Admin will ask for your password by email
- Software install requests go to **Admin / IT** — do not install from email links

If you clicked a bad link or opened a bad file

1. Stop using the PC for sensitive work

2. Disconnect from network if Admin asks
3. Tell **Admin immediately** (Level 1)
4. Change password if Admin / IT instructs
5. Do not hide the incident — early report reduces damage

How to report

- Contact: **Admin (Level 1)**
- If needed, Admin escalates to **outsourced IT (Level 2)**
- Optional: fill Incident Report Form