TRAINING 3 · HANDS-ON TRAINING

Spot and Report Phishing

Check a suspicious email step by step, safely, and report it



Cybersecurity Basics: Hands-On Training

By the end of this training you will be able to



Inspect an email safely
Without clicking anything dangerous



Check links and senders
Spot look-alike addresses and fake websites



Read email headers
Use SPF, DKIM and DMARC results



Report phishing
To your email provider, your company and in Japan

03

Training 3 of 8
Spot and Report Phishing

About 30 minutes

The golden rules



Slow down

Urgency is the attacker’s main tool. Pause before acting



Never click to check

Inspect links by hovering, not by visiting them



Verify another way

Contact the sender using a number or app you already trust

The 5-step email check



Sender

Real address, not just the name

Message

Urgency, threats, requests

Links

Hover: does the domain match?

Attachments

Unexpected? Do not open

Headers

SPF, DKIM, DMARC results

Two or more warning signs: treat the email as phishing and report it.

Real or fake? Check the address

Suspicious	What to notice
support@rnicrosoft.com	“rn” pretending to be “m” in microsoft
amazon.co.jp.account-verify.net	The real domain is the part just before the final suffix: account-verify.net
ZNexora Bank <noreply@gmail.com>	A company name on a free email address
https://bit.ly/3xYz	A shortened link hides the real destination

Step 5: Read the email headers

Check	Where	Good sign
Open the headers	Gmail: ⋮ › Show original. Outlook: … › View › Message details	Full technical details open
SPF	Authentication results	spf=pass for the sender’s domain
DKIM	Authentication results	dkim=pass with the matching domain
DMARC	Authentication results	dmarc=pass
Reply-To	Header list	Same domain as the sender

Report it

Your email app

Gmail: ⋮ › Report phishing.
Outlook: Report › Report phishing

At work

Use your company’s report button or tell IT immediately

In Japan

Forward to the Council of Anti-Phishing Japan: info@antiphishing.jp

If you clicked

Change the password, turn on MFA, and tell IT or your bank

Your checklist

- [ ] Checked the real sender address, not just the name
- [ ] Looked for urgency, threats or unusual requests
- [ ] Hovered over every link without clicking
- [ ] Did not open unexpected attachments
- [ ] Read the SPF, DKIM and DMARC results
- [ ] Verified with the sender through a trusted channel
- [ ] Reported the email and then deleted it

Check your work

1. How do you check where a link really goes without clicking it?

2. An email shows spf=fail and dmarc=fail. What does that suggest?

3. You clicked a phishing link and typed your password. What do you do next?

Answers are in the training guide.

Well done

- You can inspect a suspicious email without taking risks.
- You know how to read the technical evidence in headers.
- You know where to report phishing, at home, at work and in Japan.

Next: Training 4 · Back Up Your Data