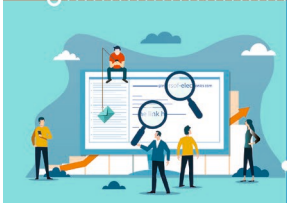


2. Don't get phished

CYBERSECURITY
SUMMER
2



DON'T GET PHISHED

Suspicious Sender Address	Generic Greetings and Language	Verify Suspicious Emails - Contact the Sender Directly - Check Official Channels - Use Anti-Phishing Tools
Urgency and Threats	Spoofed Websites	for more INFO and TIPS  Questions? ict@intersoft-electronics.com
Unusual Requests	Use of Public Email Domains	
Inconsistencies in the Email Content		
Unexpected Attachments		
Unusual Tone or Style	In summary, By staying vigilant and looking for these common signs of phishing emails, you can protect yourself from falling victim to these scams. Always double-check before clicking on links, downloading attachments, or providing any personal information in response to an email.	
Mismatched Email Address and Display Name		

1. HOW DO I RECOGNIZE A PHISHING E-MAIL?

1. Suspicious Sender Address

- Check the Domain: Phishing emails often come from addresses that look similar to legitimate ones but have slight variations, such as "support@paypa1.com" instead of "support@paypal.com".
- Unexpected Senders: If you receive an email from a sender you don't recognize, be cautious.

2. Generic Greetings and Language

- Lack of Personalization: Phishing emails often use generic greetings like "Dear Customer" or "Dear User" instead of your name. However, they can be personal as well!
- Poor Grammar and Spelling: Many phishing emails contain spelling mistakes, grammatical errors, or awkward phrasing.

3. Urgency and Threats

- Immediate Action Required: Emails that create a sense of urgency, such as claiming your account will be suspended unless you act immediately, are often phishing attempts.
- Scare Tactics: Threats of negative consequences if you don't comply quickly are a red flag.

4. Unusual Requests

- Sensitive Information: Legitimate companies will never ask for sensitive information (like passwords, credit card numbers, or social security numbers) via email.
- Unexpected Attachments or Links: Be wary of emails with unsolicited attachments or links, especially if they claim to be important documents or updates.

5. Inconsistencies in the Email Content

- Mismatched URLs: Hover over any links to see the actual URL. If the link text says one thing but the URL points somewhere else, it's likely a phishing attempt.
- Inconsistent Branding: Look for inconsistencies in logos, colors, or email format compared to previous legitimate emails from the same sender.

6. Spoofed Websites

- Lookalike Websites: Phishing emails often direct you to websites that look almost identical to legitimate sites. Check the URL carefully for misspellings or unusual domains.
- Non-Secure Sites: Legitimate sites will typically use HTTPS. If the site you're directed to doesn't have HTTPS (look for the padlock symbol in the address bar), it's a warning sign.

7. Unexpected Attachments

- Avoid Opening: Do not open attachments that you are not expecting. These can contain malware or ransomware.
- Unusual File Types: Be particularly cautious with attachments that have unusual file types (.exe, .scr, .zip).

8. Unusual Tone or Style

- Out of Character: If the email's tone or style doesn't match what you expect from the sender, it could be a phishing attempt. For example, if a colleague who usually writes formally suddenly sends a very casual email, it's suspicious.

9. Mismatched Email Address and Display Name

- Look Closely: The display name may look correct, but the actual email address could be different. Always check the full email address.

10. Use of Public Email Domains

- Public Domains: Be wary of emails from supposedly reputable companies that use public email domains like Gmail, Yahoo, or Hotmail instead of their official company domain.

2. VERIFY SUSPICIOUS EMAILS

1. Contact the Sender Directly

- If an email looks suspicious but appears to come from someone you know or a company you deal with, contact them directly using a known phone number or email address (not by replying to the suspicious email).

2. Check Official Channels

- Verify the information through official company websites or customer service channels.

3. Use Anti-Phishing Tools

- Employ email filtering and anti-phishing tools provided by your email service provider or cybersecurity software.

3. IN SUMMARY

By staying vigilant and looking for these common signs of phishing emails, you can protect yourself from falling victim to these scams. Always double-check before clicking on links, downloading attachments, or providing any personal information in response to an email.

4. MORE ON PHISHING

[Phishing: the most common attack - Knowledge Base - Intersoft Electronics \(inventive-engineering.com\)](https://www.intersoft-electronics.com/knowledge-base/phishing-the-most-common-attack)



Together we keep Intersoft Electronics cyber secure

INTERSOFT ELECTRONICS NV
Lammerdries-Oost 27 | B-2250 Olen | Belgium
Tel +32 14 23 18 11 | support@intersoft-electronics.com