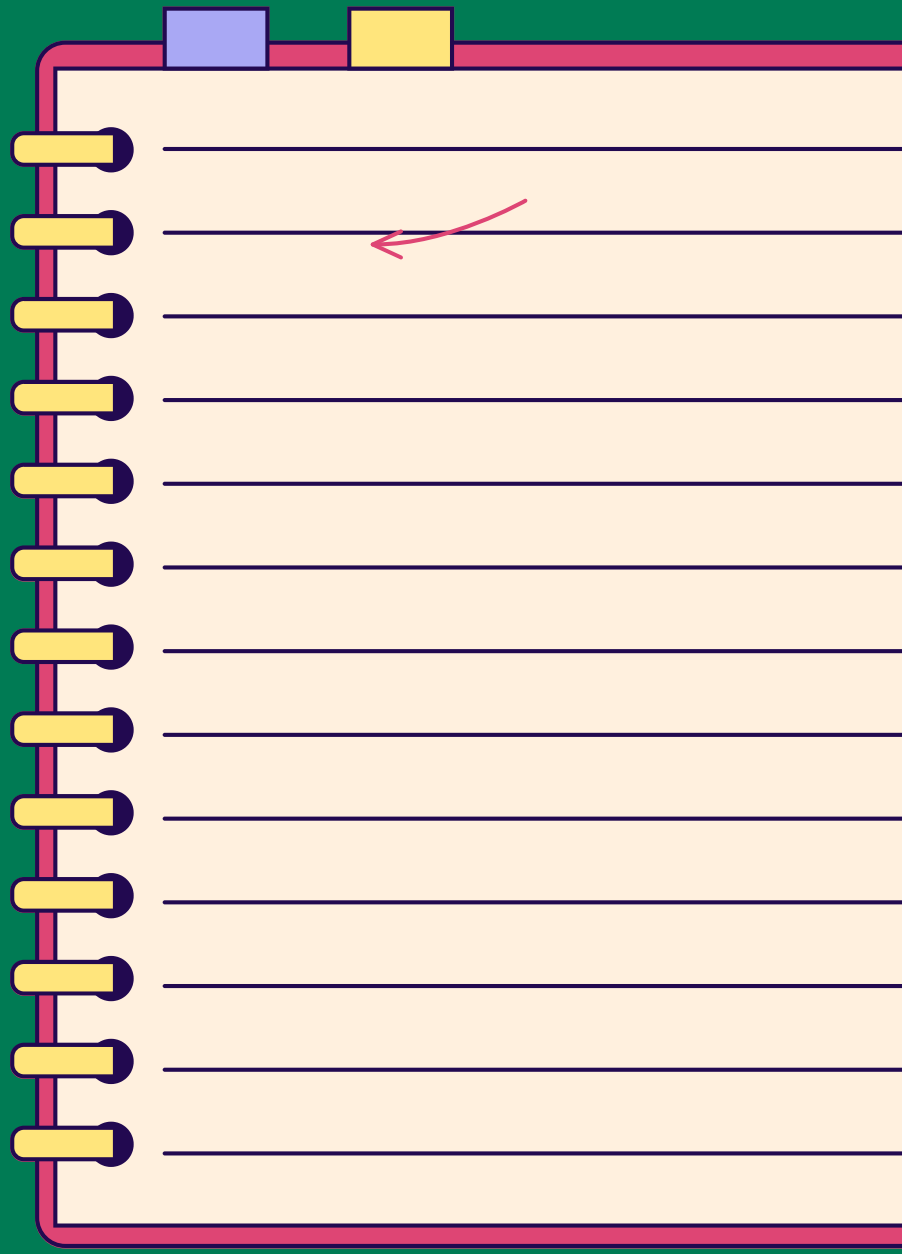
MODULE 12 - ONLINE SCAMS

CHAPTER 1

WHAT ARE THE DIFFERENT SCAMS AND HOW TO SPOT THEM?

Skills to Connect



INTRODUCTION

In the digital era, online scams are becoming more diverse and sophisticated. Whether it’s phishing, spoofing or even purchasing fraud, it’s essential to know how they work to better identify them and protect yourself from them.

In this chapter, you will discover the most common scams, how to spot them using distinctive signs, and you will learn how to adopt good practices to browse safely. At the end of this module, you will be able to detect online traps and apply the right reflexes to protect yourself from them.

1 THE DIFFERENT TYPES OF SCAM

THE PHISHING

WHAT IS PHISHING?

A technique where a malicious individual sends fraudulent messages via email or SMS, **often including a link**, to trick recipients into disclosing their personal information, **such as passwords, credit card numbers or banking information.**

Watch the video

which explains phishing and how not to get fooled!

CHARACTERISTICS OF PHISHING

- Emergency message, which plays on emotions:
  - “Your Google account has been hacked”
  - “A fraudulent money transfer has been made”
- Unusual language
  - Spelling mistakes, syntax, ...
  - Different languages (mix of English, French, etc.)
  - Specific characters? For example: è§°!µ£...
- Fake logo, wrong company name, identity theft
- You are invited to click on a link
- Strange email address or phone number, doesn't seem official

More details on the signs to look out for on page 8!

1 THE DIFFERENT TYPES OF SCAM

IDENTITY THEFT

A practice when someone or a program impersonates a trusted person by falsifying their data, such as an IP address, email address, or caller ID, to deceive victims into obtaining their personal and sensitive information.

Watch the video

which explain the scams of fake bankers

BY EMAIL

Email spoofing is a technique used in spam and phishing messages to trick targets into thinking that a message is coming from a known or trusted person or organization. Criminals alter email headers to make the sender's address appear different (and therefore familiar!) and to make the message appear authentic, especially since the email address appears to be correct.

BY WEBSITE

In website spoofing, fraudsters impersonate a trusted bank, store, or organization's website. This is often accompanied by a fake email or text message. If you click on the link in the message, you will be directed to a fake website that looks exactly like the real one. You will then be asked to enter your contact information and PINs.

BY TELEPHONE

In phone spoofing, fraudsters use an existing phone number. They pretend to be an employee of your bank, the police or another known institution and try to obtain your confidential information and codes with a lot of excuses. They then empty your bank account or ask you to make a transfer yourself. Sometimes, the fraudsters also encourage you to call a premium rate number without your knowledge. Then, they keep you on the line for as long as possible until your phone bill explodes.

1 THE DIFFERENT TYPES OF SCAM

SCAMS WHEN PURCHASING

PURCHASE FRAUD

A situation where online buyers or sellers are deceived by fictitious product listings, fraudulent e-commerce sites, or payments made but not delivered, resulting in financial losses.

Discover the article

which explains how to recognize scams on resale sites

TRIANGULAR FRAUD

A scenario where a scammer uses stolen credit card information to purchase goods from a legitimate seller, then resells those goods to an unsuspecting victim, often at a discounted price. The victim receives the product, the legitimate seller gets paid, but the real credit card holder is charged for a transaction they did not authorize.

Watch the video

which gives an example of triangular fraud

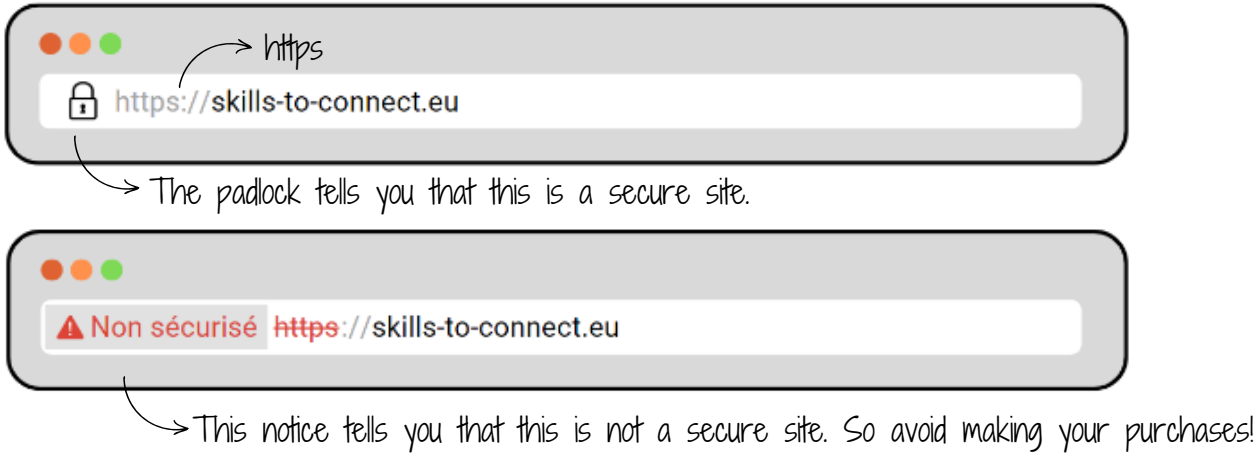
2 THE SIGNS TO LOOK OUT FOR

HOW TO RECOGNIZE A FRAUDULENT SITE

It can be hard to tell if a website is real or fake, especially if you're not used to fact-checking. Here are some **simple tips** to help you spot scam sites:

CHECK THE SECURITY OF THE SITE, USING SEVERAL SIGNS:

Check the website address (or URL), which is located at the top of your browser in the address bar. A secure site always begins with "https://". The "s" stands for "secure". You should also see a small padlock next to the address.
Be careful of addresses that look like real sites but with mistakes or additions!



Also check the domain name!
Fraudsters often copy the addresses of well-known sites, changing just a small detail.

- Real site: https://www.amazon.com
- Fake site: https://www.amaz0n-shop.com (a "0" replaces the "o").

2 THE SIGNS TO LOOK OUT FOR

HOW TO RECOGNIZE A FRAUDULENT SITE

OBSERVE THE DESIGN AND CONTENT OF THE SITE

like the example on page 15!

- On a real website, everything is often well presented: the texts are clear, without errors, and the images (like the logos) are of good quality.
- On a fake site, you will often find spelling mistakes, blurry logos, or a design that "looks weird." Sometimes, some links don't work.

LOOK FOR CONTACT INFORMATION

- A serious website displays its contact details: address, telephone number, and sometimes a contact form. You will often find this information at the bottom of the page (in the "legal notices").
- If this information does not exist or seems strange (for example, a simple email like contact@gmail.com), be wary.

BEWARE OF OFFERS THAT SEEM TOO GOOD TO BE TRUE

- If a product costs significantly less than anywhere else (for example, an iPhone for 100 euros), there is a good chance that it is a scam.

Tip: Compare prices on other popular sites to see if it seems realistic.

LOOK AT THE PAYMENT METHODS OFFERED

- Real sites use secure payment methods, such as credit cards or PayPal.
- Be careful if they ask for a bank transfer, cryptocurrency payment, or other unusual payment method. Once the money is sent, you often won’t be able to get it back.

2 THE SIGNS TO LOOK OUT FOR

HOW TO RECOGNIZE A FRAUDULENT SITE

OBSERVE THE DESIGN AND CONTENT OF THE SITE

- Before trusting a site, Google its name followed by the word "review" or "scam."
- Type in "shoppingtech.fr reviews" to see if other people have had problems.
- Check out trusted review sites like:
  - Trustpilot: is a review platform where users share their experiences with companies, whether positive or negative.
  - Scamadviser: a collaborative site dedicated specifically to reporting scams and frauds, allowing other users to be alerted to potential fraud.

→ Use these tools to check the reliability of your site! If you see a lot of comments saying "order never received" or "payment taken but nothing received", it is probably a fake site.

BE CAREFUL OF ADS AND POP-UPS THAT POP UP EVERYWHERE

- Fake sites often contain ads everywhere. If you see windows that open all the time or messages telling you that you have won a prize, close everything and leave the site.

2 THE SIGNS TO LOOK OUT FOR

HOW TO RECOGNIZE A FRAUDULENT MESSAGE

Scams can come in the form of emails, text messages, or even phone calls. Fraudsters are trying to trick you into giving up your personal information. Here's how to spot them:

THE SENDER'S ADDRESS OR SUSPICIOUS NUMBER

Fraudsters often use fraudulent addresses or numbers. There are a few signs to spot to make sure the person you are talking to is not a scammer:

SPOTTING A FRAUDULENT EMAIL ADDRESS:

Fraudsters often use email addresses like official companies, but with small errors. For example, instead of support@bank.com, a fraudster might use bank-support@mail.com. This can be hard to see at first glance, but if you look closely, you can spot the difference.

If the email address looks strange or contains spelling misktakes, it is probably a scam. Always check the address on the company's official website before responding.

SPOTTING A FRAUDULENT CALL:

Fraudulent calls can come from unknown numbers or withheld numbers (where no number appears on your phone). Fraudsters can also use numbers that look like those of businesses, but have a slight difference. For example, a call may appear to be from your bank, but the number displayed is not the one you are used to seeing.

If the call comes from a hidden or unknown number, or if the number does not match the company's number, it is best not to answer. Contact the company directly using official information to verify if the call was legitimate.

2 THE SIGNS TO LOOK OUT FOR

HOW TO RECOGNIZE A FRAUDULENT MESSAGE

SPOTTING A FRAUDULENT SMS

- Some companies use short numbers or special numbers like 8000, 8080 or others to send official SMS messages, such as alerts or promotions. However, scammers can also use these numbers to hide their real identity and deceive you.
- If the text message comes from an unknown short code or a strange number (for example, a number starting with +44 or +1), or if the content seems too urgent or too good to be true, it is probably a scam. For example, a text message claiming to be from your bank but asking you to click on a link or provide sensitive information is suspicious.

If you don't recognize the number or the message seems suspicious, do not respond or click on any links. Contact the company directly through its official number to verify.

THE MESSAGE IS STRANGE

Fraudulent messages, whether they come via email, text message, or even phone call, often contain grammatical errors, syntax mistakes, or awkward wording. These errors are a sign that it is likely a scam attempt.

MESSAGES PRETENDING TO BE FROM A COMPANY:

A message that starts with “Dear User” instead of using your first name or “Hello Sir/Madam” is suspicious. Legitimate businesses, such as banks or e-commerce sites, typically personalize their messages by including your name in the subject line or body of the text. If you don’t see your name or the message is too generic, that’s a red flag.

- **FRAUDULENT: DEAR USER, YOUR ACCOUNT WILL BE SUSPENDED.**
- **LEGITIMATE: HELLO ___, WE HAVE AN UPDATE REGARDING YOUR ACCOUNT.**

2 THE SIGNS TO LOOK OUT FOR

HOW TO RECOGNIZE A FRAUDULENT MESSAGE

MESSAGES PRETENDING TO BE PUBLIC OR GOVERNMENT SERVICES:

If you receive an SMS or email that appears to come from a public service (for example, tax or social alerts), but with spelling mistakes, this is a big alert. Official messages from administrations are generally written in a neat and professional manner. Fraudsters sometimes try to pass themselves off as public institutions, but they do not always take care of the quality of their writing.

- ✗ **FRAUDULENT: THE TAXMAN OWES YOU MONEY, CLICK HERE TO CLAIM YOUR FUNDS**
- ✓ **LEGITIMATE: THE TAX DEPARTMENT INFORMS YOU THAT YOU ARE ENTITLED TO A REFUND. FOR MORE INFORMATION, LOG IN TO YOUR PERSONAL SPACE**

MESSAGES PRETENDING TO BE FROM A FRIEND OR CONTACT PERSON

Sometimes scams can appear to come from friends or contacts you know, especially if their account has been hacked. If a message from your friend seems strange, has typos, or has an unusual tone (e.g., “I found a great deal for you!”), it could be a phishing attempt.

- ✗ **FRAUDULENT: HEY, CHECK OUT THIS AWESOME VIDEO, I THINK YOU'LL LIKE IT!**
- ✓ **LEGIT: HI___, I'M SENDING YOU THE VIDEO I TOLD YOU ABOUT, WATCH IT WHEN YOU HAVE A MOMENT 😊**

2 THE SIGNS TO LOOK OUT FOR

HOW TO RECOGNIZE A FRAUDULENT MESSAGE

THE MESSAGE IS URGENT

Scammers often try to get you to react quickly by putting pressure on you, using urgent or threatening messages.

URGENT MESSAGES

You may receive a message telling you that your account will be blocked or that you need to take immediate action to avoid a problem:

- **YOUR ACCOUNT WILL BE SUSPENDED IN 24 HOURS!**
- **REPLY NOW TO AVOID ACCOUNT CLOSURE**

OFFERS TOO PRESSING

Sometimes scammers tell you that you have won a prize, but that you must act immediately to receive it:

- **YOU HAVE WON 1000€, CLICK HERE BEFORE TONIGHT TO COLLECT IT!**

OFFERS TOO PRESSING

They may also try to scare you with threats of fines or legal action if you don't respond quickly.

- **YOU MUST PAY THIS FINE WITHIN 48 HOURS, OTHERWISE YOU WILL BE PROSECUTED!**

THE MESSAGE ASKS FOR YOUR PERSONAL DATA

- If a message asks you for sensitive information, such as your password, credit card numbers, or PIN, it's a clear sign of a scam.
- **No serious company will ask you for this information by email, SMS or phone!**

2 THE SIGNS TO LOOK OUT FOR

HOW TO RECOGNIZE A FRAUDULENT MESSAGE

THE MESSAGE ASKS FOR YOUR PERSONAL DATA

- If a message asks you for sensitive information, such as your password, credit card numbers, or PIN, it's a clear sign of a scam.
- **No serious company will ask you for this information by email, SMS or phone!**

GOOD TO KNOW

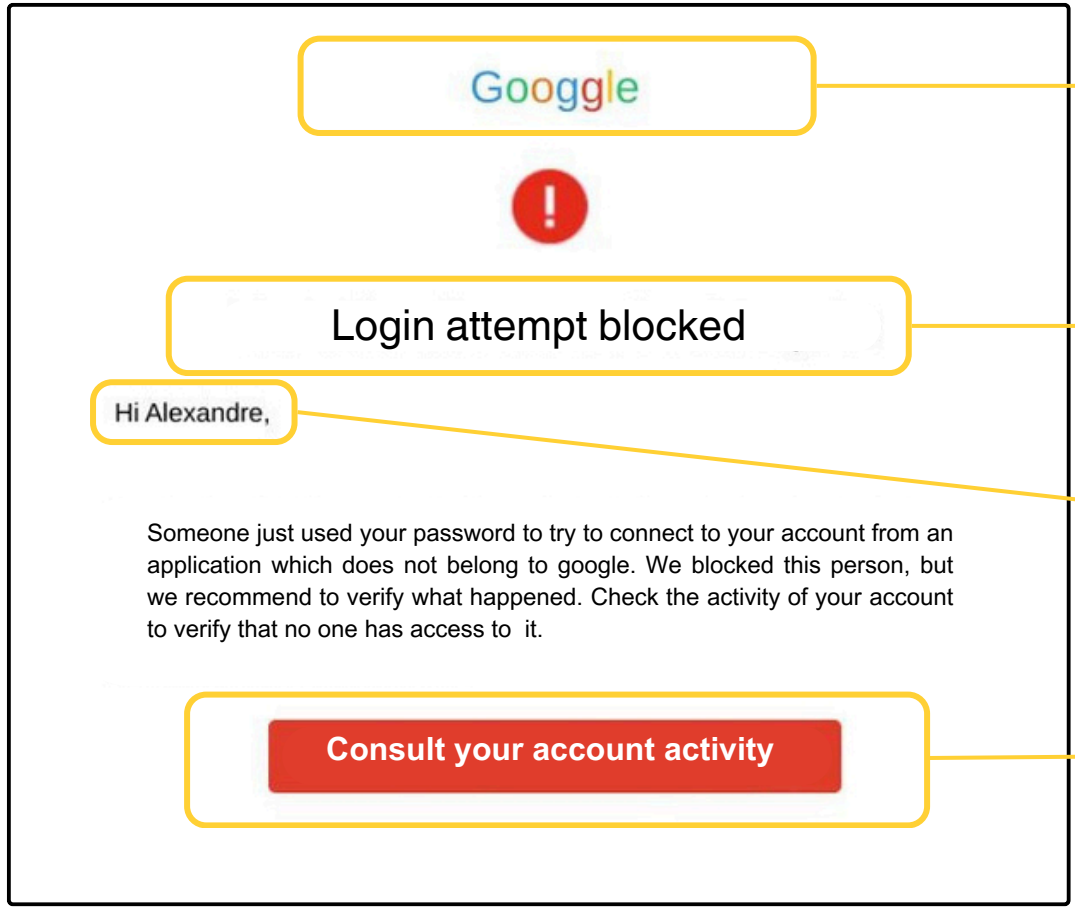
- A bank advisor will never ask you for your sensitive personal information, such as your password, over the phone. Banks do not need your password to access your information or help you with a problem. If you receive a call from an advisor asking for your password or other confidential information (such as your PIN or credit card number), it is likely a scam attempt. Do not answer and contact your bank directly using the official contact details.

- To access online public services in **Belgium**, you must log in via the CSAM platform (Belgian government services platform) or ITSME, a security application. For example, you will never receive official communication about your taxes by email. You consult your taxes on the MinFin platform. If you receive an email asking you to click on a link to access your tax return, this is a phishing attempt. This type of fraud can also concern other public services, such as Ma Pension or other government services. Be vigilant and never click on a suspicious link in an email.

2 THE SIGNS TO LOOK OUT FOR

HOW TO RECOGNIZE A SCAM

PHISHING EXAMPLES



Fake logo

the real google logo looks like this

Google

Emergency message

Plays on emotions, stress and a sense of urgency to push you into action without thinking

Unusual

Mix of English and French

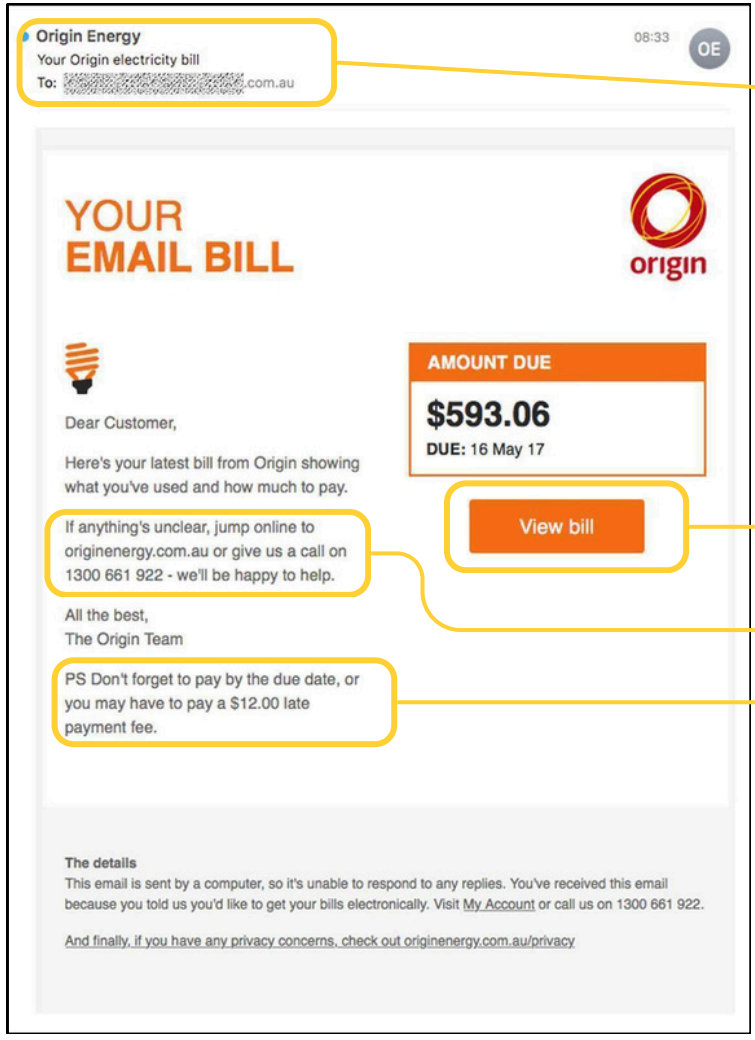
Push to action

A fraudulent link is hidden behind the button

2 THE SIGNS TO LOOK OUT FOR

HOW TO RECOGNIZE A SCAM

PHISHING EXAMPLES



Strange mail name

Emergency message

Plays on emotions, stress and a sense of urgency to push you into action without thinking

Fraudulent link

The link and the phone number are not secure and surely a scan you can verify them! before clicking

Push to action

A fraudulent link is hidden behind the button!

TO REMEMBER!

Online scams come in many forms, including phishing, spoofing, and online shopping fraud. It's important to be vigilant about these fraud attempts. A telltale sign of a scam can be a message that asks for personal information or that seems too urgent or too good to be true. Always double-check the email address, phone number, and links in messages. Grammar mistakes or a threatening tone are often indicators of fraud. Finally, if you have any doubts, don't hesitate to contact the company or organization directly through an official channel to verify the legitimacy of the message. **Protecting yourself against these scams starts with knowing how to recognize them!**