

Phishing e-mail awareness training

By Daniel Ellebæk, 2021 June

[Security-in-mind.com](https://www.security-in-mind.com)



Agenda

- Statistics
- What is a phishing e-mail?
- Seven ways to detect a phishing e-mail
- Phishing e-mail examples
- What if it all checks out
- The phishing attack case from earlier
- What to do if you clicked or downloaded content from a phishing e-mail?

Who am I?

Daniel Ellebæk



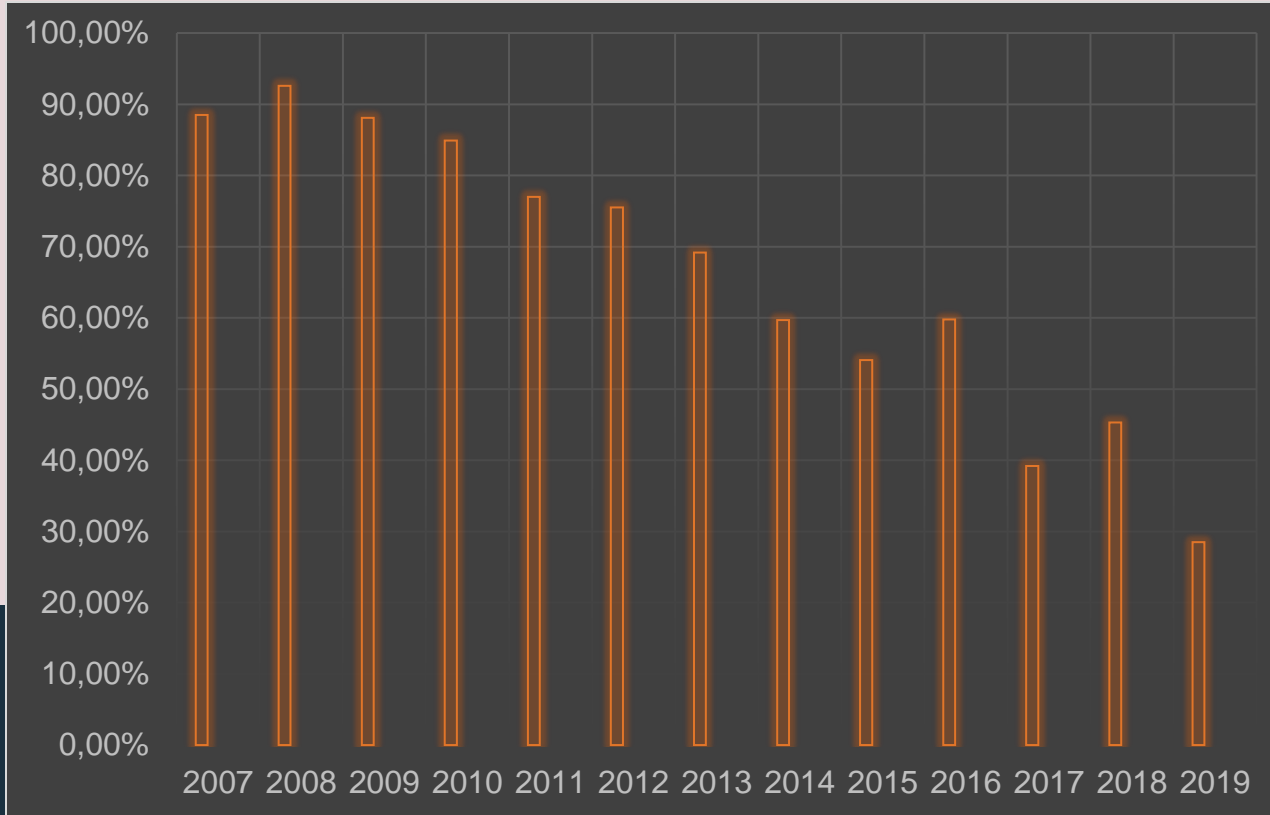
Worked actively with Cyber
Secyurity since 2014

Started working
@Cphbusiness Lyngby august
2020



Statistics

Global spam volume as percentage of total e-mail traffic from 2007 to 2019



Phishing facts from 2020-2021

01

Less common

Credential Phishing

02

More common

Key loggers 70%+ of all attacks

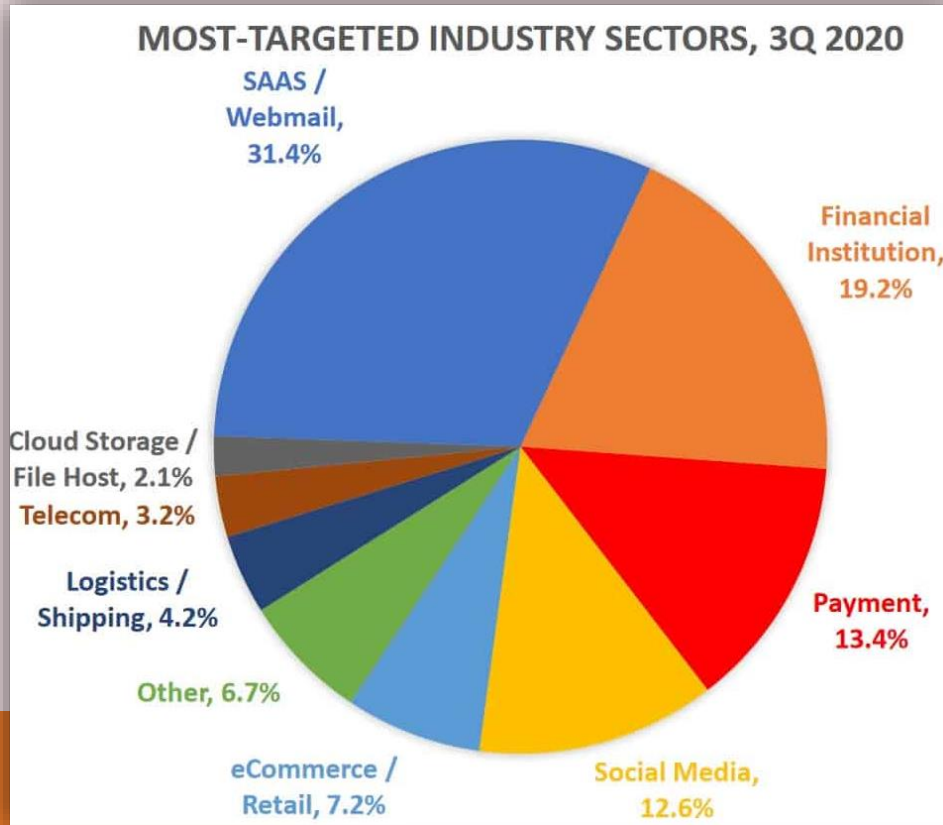
03

Last year

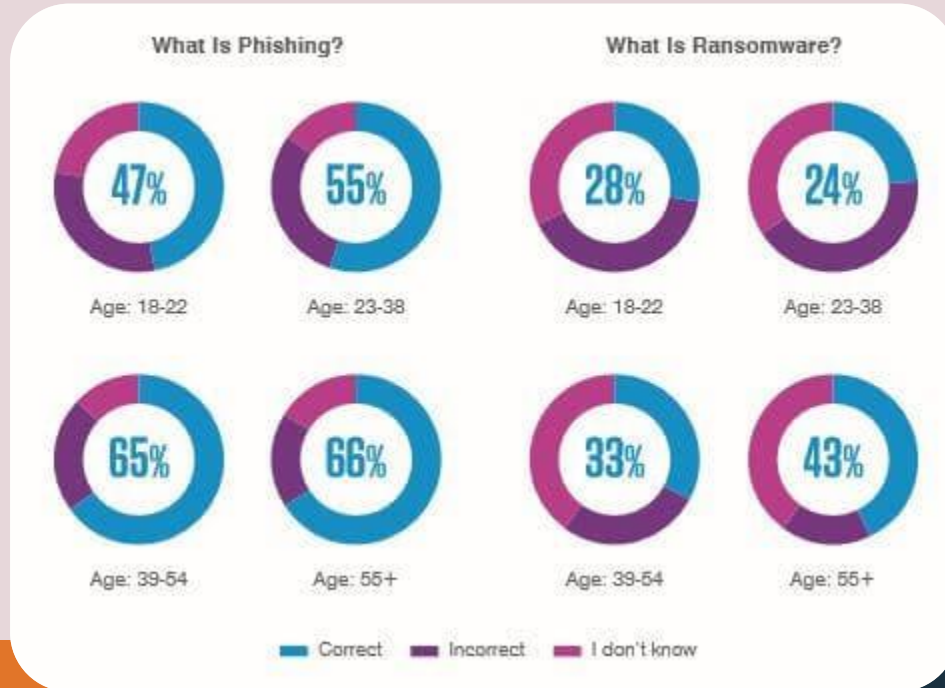
74% of all attacks was stealing usernames and passwords



Most targeted industry sectors 2020+

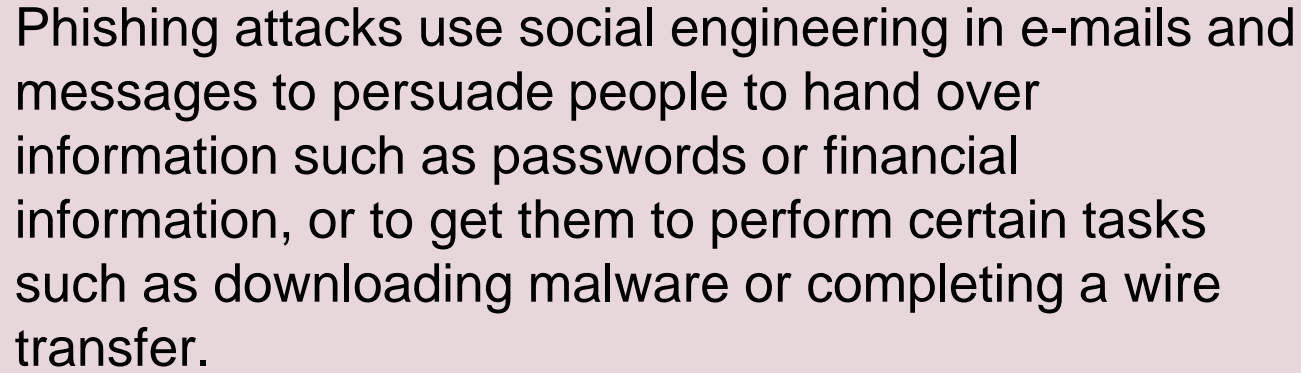


Knowledge of phishing terms varies among generations





What is a phishing e-mail?



Phishing attacks use social engineering in e-mails and messages to persuade people to hand over information such as passwords or financial information, or to get them to perform certain tasks such as downloading malware or completing a wire transfer.

—What is a phishing e-mail





Seven ways to detect a phishing e-mail

Legit companies don't request your sensitive information via email.

—Method #1

Legit companies usually call you by your name.

—Method #2

Legit companies have domain emails.

—Method #3

Legit companies know how to spell

—Method #4

Legit companies don't force you to their website (e.g., e-mail is a giant hyperlink)

—Method #5

Legit companies don't send unsolicited attachments (e.g., not expected attachments)


—Method #6

Legit company links match legitimate URLs

—Method #7



Phishing e-mail examples

From: GlobalPay <VT@globalpay.com> 
Subject: Restore your account
Date: February 7, 2014 3:47:02 AM MST
To: David

[Hide](#)

1 Attachment, 7 KB

Save ▼

Quick Look

Dear customer,

We regret to inform you that your account has been restricted.

To continue using our services please download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc



[update2816.html \(7 KB\)](#)



Hotels.com <Hotelscom@roktpowered.com>
to dave ▾

Nov 14, 2018, 11:38 AM (1 day ago)



[Hotels](#) [Hotel Deals](#) [Packages & Flights](#) [Groups](#) [Customer Service](#) [Gift Cards](#) [Secret Prices](#)



[New York Hotels](#) [Las Vegas Hotels](#) [Chicago Hotels](#) [Los Angeles Hotels](#)

COUPON CODE

\$50 off

When you spend \$350 or more

EMLRKUSH21850:SK7CM6 [Book now](#)

You must click through this email or book through our app to redeem this coupon.

*Use by 11:59 PM MT on 01/15/19 for travel by 04/30/19. Can't be used on some hotels. See details below.

Bookings using this coupon are not eligible for Hotels.com™ Rewards.

Hide

From: Costco Shipping Agent <manager@cbcbuilding.com>
Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbcbuilding.com>



Unfortunately the delivery of your order [COS-0077945599](#) was cancelled since the specified address of the recipient was not correct. You are recommended to complete [this form](#) and send it back with your reply to us.

Please do this within the period of one week - if we dont get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.

From: **Best Buy** <BestBuyInfo@fashionlab.com.ua>
Subject: Special Order Delivery Problem
Date: December 20, 2013 11:06:08 AM MST
To: dave
Reply-To: Best Buy <BestBuyInfo@fashionlab.com.ua>

[Hide](#)

My Best Buy ID: 002024460
Reward certificate(s) available.



WEEKLY DEALS

GIFTS

Tvs

Computers & Tablets

Cell Phones

Appliances

Cameras

Video Games

Audio


Sir/Madam,

Your order [BBY-4983814314](#) has not been delivered because the specified address was not correct. Please fill this [form](#) and send it back with your reply to this message.

If we do not receive your reply within a week we will pay your money back less 17 because your order was reserved for the time of Christmas holidays.

Best Buy 7601 Penn Avenue South, Richfield, MN 49584-7655

BEST BUY, the BEST BUY logo, the tag design, [BESTBUY.COM](#), GEEK SQUAD, the GEEK SQUAD logo, MY BEST BUY, REWARD ZONE, BEST BUY MOBILE and the BEST BUY MOBILE logo are trademarks of BBY Solutions, Inc. All other trademarks or trade names are properties of their respective owners.

From: Manager Daniel Bridges <daniel_bridges33@gulfslipformpaving.com> 
Subject: Information
Date: August 26, 2013 1:25:12 AM MDT
To: dave
Reply-To: Manager Daniel Bridges <daniel_bridges33@gulfslipformpaving.com>

USPS.COM

Notification

Our courier couldnt make the delivery of parcel to you at 20th August.
Print label and show it in the nearest post office.

[Print a Shipping Label NOW](#)

From: "Bank" <payment@epayment.com>

Subject: Re: new payment on your account

Date: March 24, 2014 10:39:01 AM MDT

Reply-To: <bankwiretransferdepartment@gmail.com>

Please find attached bank slip for new payment on your account.

Regards,

Account Department.



new payment.zip

From: **Nokia** <info@news.nokia.com>
Subject: **SAVE YOUR STUFF!** Sign in to your Nokia account before it disappears forever!
Date: February 7, 2014 2:38:02 AM MST
To: :
Reply-To: **Nokia** <info@news.nokia.com>

[Hide](#)

NOKIA

SAVE YOUR STUFF!

We noticed you haven't used your Nokia account to access Nokia services in quite a while. To protect your privacy, this account will be deleted in 14 days, [so sign in now](#).

If you haven't experienced Nokia services recently, they're worth another look. And you may want to keep any maps, locations, email, music, reviews, or other stuff that is associated with your account.

It just takes a few seconds to [sign in to your Nokia account](#).

We hope to see you soon.

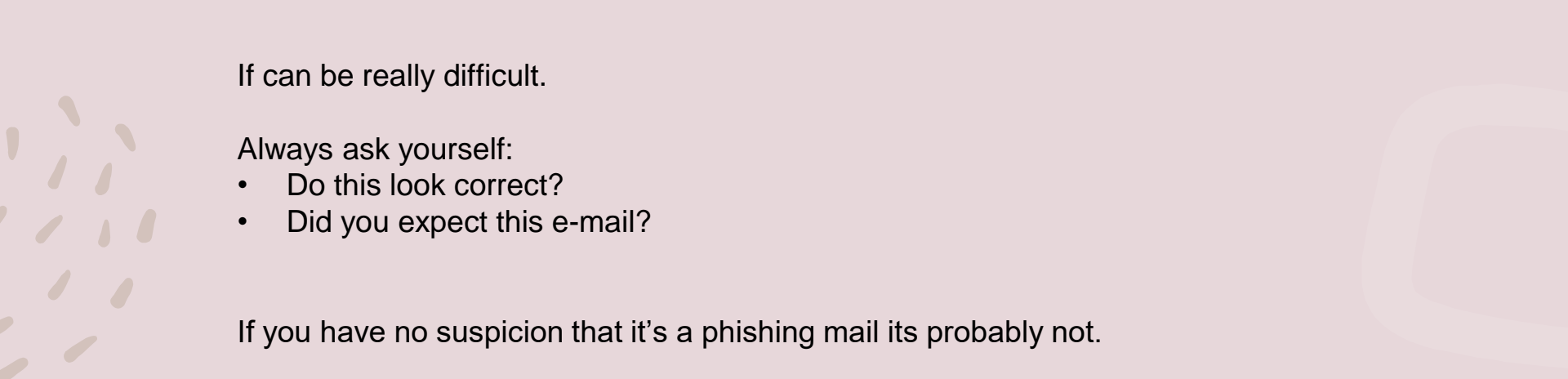
Sincerely,
The Nokia account team

[Privacy policy](#) | [Terms and conditions](#) | [Support](#) | [Contact us](#)
Nokia Corporation P.O. Box 226 FI-00045
Nokia Group Finland

© 2014 Nokia



what if all checks out...
how can I verify whether it's a
phishing e-mail or not...?



If can be really difficult.

Always ask yourself:

- Do this look correct?
- Did you expect this e-mail?

If you have no suspicion that it's a phishing mail its probably not.

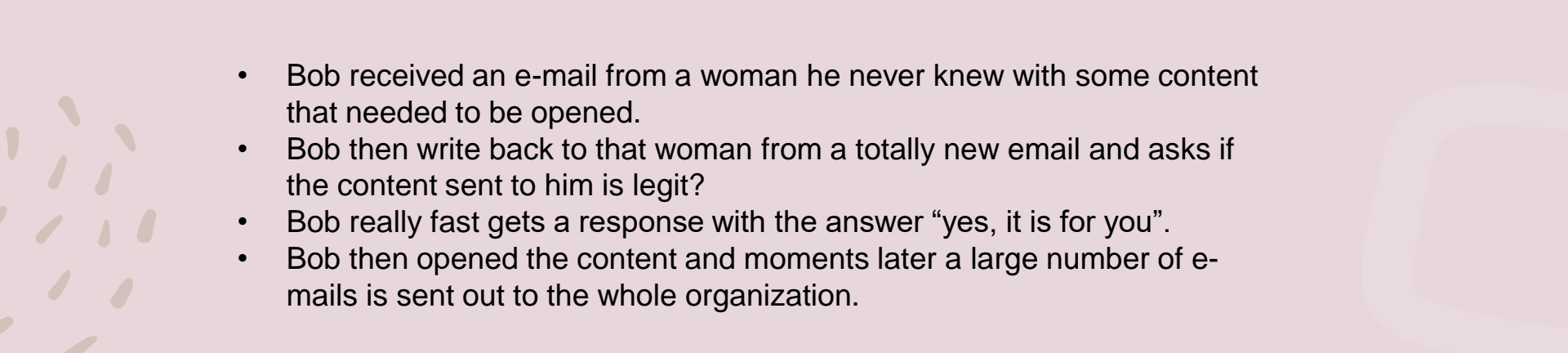
Open it.

—Common sense





The case that happened not too long ago...

- 
- Bob received an e-mail from a woman he never knew with some content that needed to be opened.
 - Bob then write back to that woman from a totally new email and asks if the content sent to him is legit?
 - Bob really fast gets a response with the answer “yes, it is for you”.
 - Bob then opened the content and moments later a large number of e-mails is sent out to the whole organization.

The woman's e-mail was compromised. Even if you can get a response back many people would say “its safe now, I can trust the content” because I got told to trust it.

People are eager to trust others.



It can be this real...



What can happen if you **click a link in
a phishing email **or open attached**
content?**

Clicked a link or open attached content

- **[link]** Coding that uniquely identifies you. That you read your email and clicked a link. A better scammer then might try and trick you even further. You will then be a higher profile target. Sell your e-mail to a good price. At best you will get more spam.
- **[Open attached content]** Might directly try to compromise your computer. Though many attachment do contain links to avoid your spam filter and/or virus scanner.
- **[link]** might infect your computer or browser with malware.
- **[link]** or **[Open attached content]** Ransomware (your files locked until you pay)
- **[link]** or **[Open attached content]** Trojans (your computer wide open for data theft etc.)
- **[link]** or **[Open attached content]** Bots (enslave your computer to work for the scammers)

And a lot more...



What to do if you clicked or downloaded content from a phishing e-mail?

If you clicked a phishing e-mail

Change password

Change your passwords

- The compromised
- If you can do it from another device than the compromised



Run virus scanners (offline)

Turn off your internet

- Run scanners



Tell the IT department

Inform the IT department that you been compromised

- Do it from your phone at best



In some cases, you might need to get your machine re-installed

If you downloaded content

Run virus scanners (offline)

Backup - but to a USB or external drive

- Run scanner on the device later



Change password & change all passwords

- The compromised
- Reinstall PC (safest)



Tell the IT department

Inform the IT department that you been compromised



- Do it from your phone at best



In some cases, you might need to get your machine re-installed



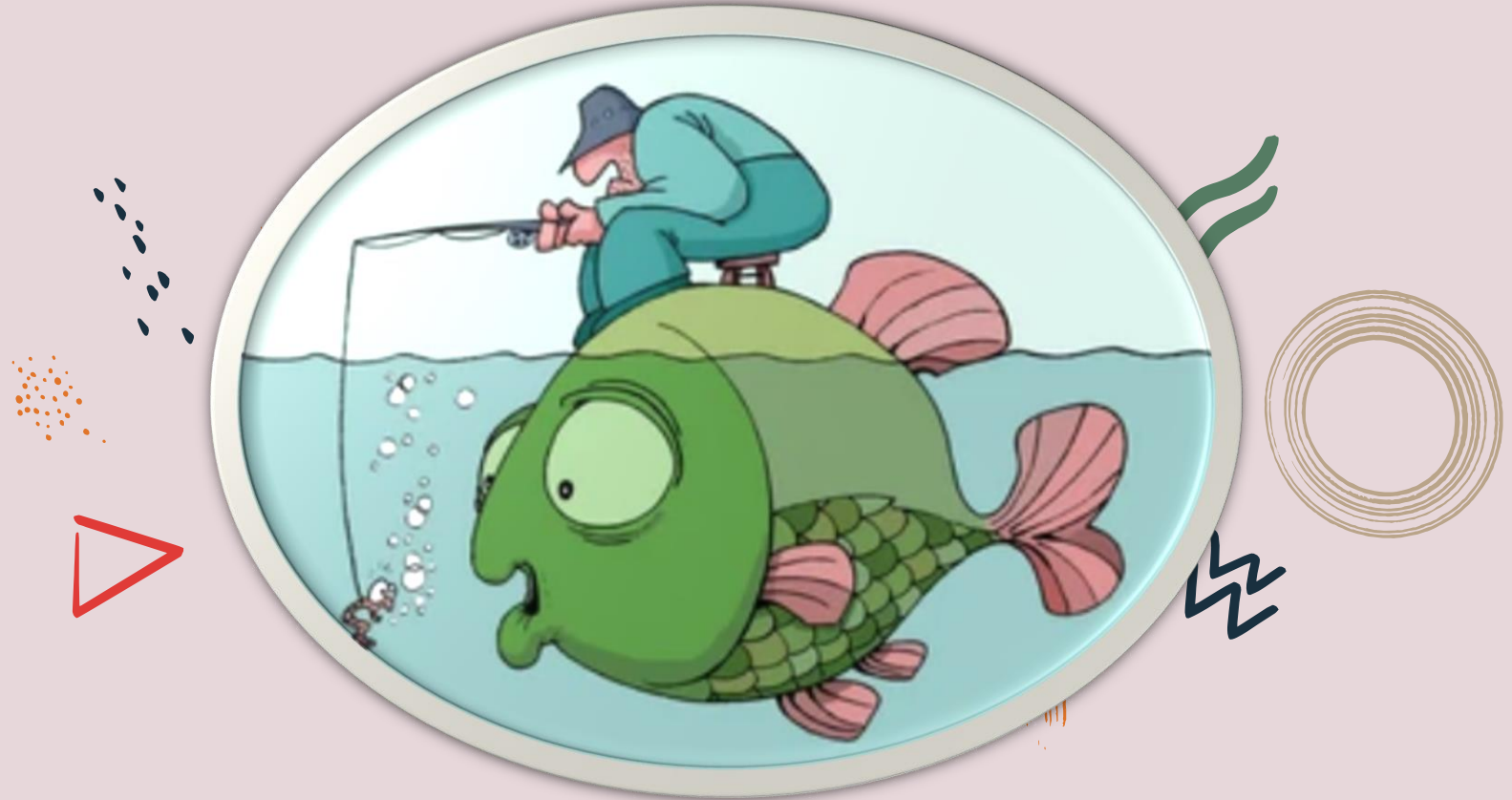
Recommendations in general

- 
- 
- Use MFA (multi factor authentication) to your e-mail account (if possible)
 - When you receive an e-mail with a link that you are not sure about....
Delete it
 - Choose a password that is 16 characters or more long. Focus on length over complexity.



Recommendations

Thanks for listening



Sources

https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf

<https://www.statista.com/>

<https://www.youtube.com/watch?v=gqhPkeXMeh0>

Online Phishing Test

<https://www.phishingbox.com/phishing-test>

Online password strength

<https://www.security.org/how-secure-is-my-password/>

List of free scanners

<https://www.antivirussoftwareguide.com/free-virus-scan>