

We can help you stop phishing.

# Retarus Anti-Phishing Guide

---

Phishing emails that have made it to your inbox despite email security have a strong adversary. That's you.

Learn how you can protect yourself and your company from online fraud.



# Be alert.

---

Expect an online fraud attempt at any time. The likelihood that you will fall into a phishing trap is reduced immensely if you are aware.

**i** Phishing is online fraud in which cyber criminals try to spread malware, intercept data, and gain financial benefits. Cyber criminals use false identities and manipulative messages that exploit typical human characteristics such as good faith, readiness to help, or fear (social engineering).



## **Online scammers often disguise themselves as close acquaintances.**

Online scammers pretend to be friends or family members. Or they take on the role of colleagues, managers, or business partners and pretend to be acting on behalf of official institutions, established financial service providers, or online portals (e.g., your bank, PayPal, Amazon etc.).



That means that even if you “know” the sender of an email, it could be a phishing attempt.

## **The quality of phishing attempts is getting better and better all the time – technically, optically, and from a content perspective.**

We are seeing fewer and fewer phishing emails with never-ending cryptic links and clumsy instructions in poorly written English and a bad design. The latest generation of phishing emails are technically sophisticated, well-written, and professionally designed.




Fake emails, manipulated senders, attachments, downloads, and websites often appear surprisingly real and, at second glance, are not immediately recognizable as fake.



# Be cautious.

---

If you have the feeling that there is something strange about an email or a website, be cautious. If you suspect a phishing attack, the best thing to do is to not respond.

 Cyber criminals hide malware in attachments, links, and download options. These can paralyze not only your computer, but – in a worst-case scenario – your entire IT infrastructure.



**#1** Never click on links in suspicious emails (do not click on unsubscribe links either\*).

---

**#2** Do not open/download attachments to suspicious emails (malware).

---

**#3** Do not reply\* to a suspicious email and do not forward it.

---

**#4** Never enter your user name, password, or other personal data on websites that look suspicious.

---

\*This will only confirm your email address.

### **Warning! CxO fraud!**

CxO fraud is a particularly brazen phishing method in which cyber criminals pretend to be managers and urge their employees under false pretenses (e.g., emergency situations) to do something (e.g., transfer money or disclose confidential information).

Typical phishing emails of this type appear to be urgent and ask you to treat the request confidentially.

### **Do you know the sender of an email with suspicious content?**

Check the authenticity of the email by speaking with or calling the sender.

### **Do you think that you've fallen into a phishing trap?**

Don't waste a single minute. Contact your manager and/or your IT department so they can explain what to do next.

# Be skeptical.

---

Online scammers see trending information in the general public as an opportunity for cyber-crime. That's why they often use topics that affect us personally, that are covered intensively by the media, or that fill us with concern or joy as "lures".



Note that scammers are not just targeting us via email and on websites. They are also active on social media, via text, over the phone, and even at your doorstep.



Be skeptical when an offer arrives “on cue” or seemingly perfectly timed, a message seems to particularly appeal to you, or the communication involves home-office instructions. It’s best to take a moment and observe the thoughts and feelings a message triggers in you. Does a routine, a principle, or a general rule “guide” you? Does an authority “speak” to you? Does a fear resonate? Is an all-too-perfect opportunity beckoning? If so: take a deep breath, think again, do some research - and only then make the choice to react or not.

## How cyber criminals are trying to spread malware, intercept data, and make money:

**Official, indispensable or exclusive information** in the form of a newsletter subscription, email attachment, or as a download option

**Unique opportunities** such as offers for products that are in high demand or only available for a limited time, high chances of winning, investment tips, ...

**Data queries/data matching of online accounts** (employees, customers, users, members, patients, ...)

**Instructions** and requests that put the reader **under pressure** (e.g. relating to distress, omission, danger, ...)

**Downloads or installation** of software or security updates

**Password requests** for participating in video conferences

**Data queries/data matching** for activating a **remote tool** (remote maintenance)

---

**Are you suspicious of IT instructions you’ve received regarding your home office?** Check with your IT department each time to be sure they are legitimate.



## The one true way to fight phishing: solid email security and awareness!

Be alert and expect online scamming at any time.  
Be cautious and avoid clicking or downloading  
spontaneously. Be skeptical and question what  
might be behind the message, use common sense,  
and rely on more than one source of information.

---

### Retarus Email Security

Ensuring that email in your company keeps running  
and does not come to a halt.

[retarus.com/email-security](https://retarus.com/email-security)

