FREEDOM BROKER

HOW TO RECOGNIZE TELEPHONE FAKERS

and not to fall for their tricks

How to understand that fakers are calling

They request confidential information, including bank card details, information about financial transactions, personal data, passwords, logins, and so on.

They rush and create panic. You need to act immediately, otherwise

They create an artificial threat. They are afraid of losing money, legal, financial and credit consequences that can be avoided, if their requirements are met.

They use complex terminology They refer to non-existent laws and banking procedures to confuse.

What can fakers take advantage of?

Uncertainty. If you do not know much about banking or are not sure how services should work, fakers can take advantage of this.

Desire quickly and easy to earn. If you are promised easy money, such as a big win or an unexpected bonus, this could be a trap.

Absent-mindedness. If you are busy or in a hurry, fakers may try to confuse you or force you to do something rash.

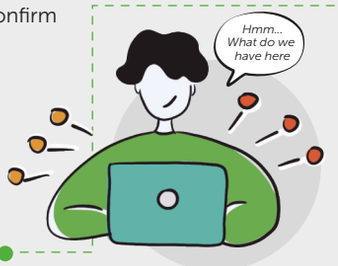
Fear of losing money. If you are told that your savings are at risk and you need to do something urgently, this can be a way to force you to act without thinking.

How to protect oneself from phone fakers

1 **Check any information.** If you receive a call on behalf of a bank or other organization, do not rush to comply. It's better to call the company's official number to confirm this information.

2 **Don't be afraid to refuse.** Confident refuse any proposals or demands, if they are in doubt.

3 **Don't act under pressure.** Do not make any transactions or provide personal information, if you feel pressured or panicked.



4 **Study the methods of scammers.** Read about how scammers operate to be aware of the main fraud schemes.

5 **Do not provide confidential information.** For example, passwords or PIN codes. Respectable companies and services will never request such information, because it contradicts digital security requirements.

6 **Do not install software or applications using someone's request.** Especially, if this is a call from an unknown number.

FREEDOM BROKER

HOW TO RECOGNIZE PHISHING SCAM LETTERS

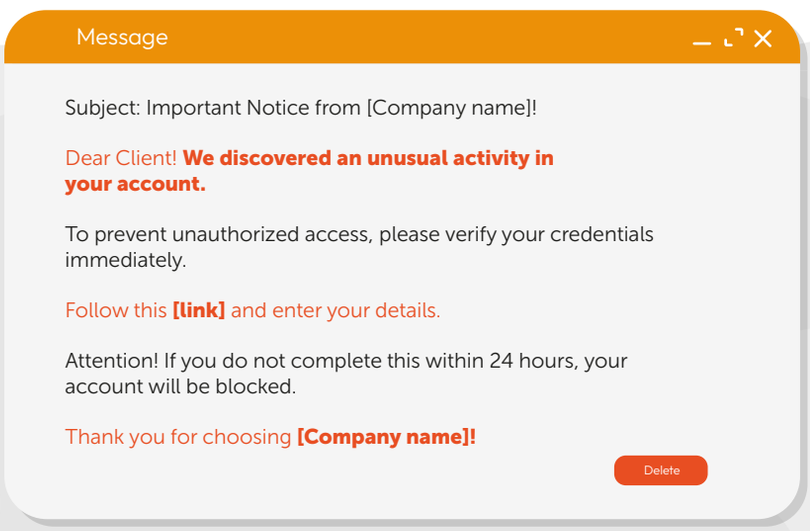
and defend oneself from online fraud

What are phishing scam letters?

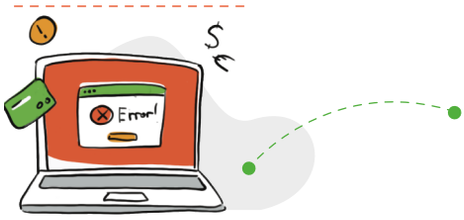
These are false messages that look like official letters from financial institutions, services, or even your friends.
The purpose of such letters is to steal your personal information (for example, passwords and bank card numbers).

How do phishing scam letters look like?

1. They usually contain requests to urgently confirm something, change a password, or update account information.
2. The letters may contain links leading to fake websites where you will be asked to enter personal information.
3. Sometimes, these letters may contain grammatical errors (to bypass spam filters).



Common fraud schemes



False messages about account blocking.
Fraudsters claim that your account is blocked and ask you to enter personal information to restore it.

Requests for help.
Fraudsters may pretend to be your acquaintances and ask to transfer money, supposedly for urgent help.

Offers to win or inheritance.
They may write to you about an unexpected win or inheritance, but to receive it you will have to pay or provide personal information.

How to protect oneself

Don't follow suspicious links.
If you receive a strange letter, it is better not to click on the links inside it.
yes

Check the address sender.
If the address email looks unusual, it could be a phishing scam letter.
yes

Use two-factor authentication.
This is an additional level of protection for your accounts.
yes

Don't share personal information. Never enter your passwords, card details or other important information anywhere, if you are not sure of reliability of the source.
yes

Use an antivirus.
Update your computer's antivirus software regularly.
yes

Be careful.
If the letter seems suspicious, it is better to double-check the information by calling the financial organization directly.
yes

Remember: It's always better to be safe and check the information than face the consequences of fraud. Be vigilant and careful, when communicating on the Internet.

FREEDOM BROKER

HOW TO RECOGNIZE PHISHING WEBSITES
and protect oneself from them

What are phishing websites?

These are fake web pages created to steal personal data (logins, passwords, bank card numbers and other confidential information). Such websites may imitate popular pages and services to trick users into entering personal information.

- Internet banking
- Social media
- Email Login Pages
- Online stores
- Trading platforms
- Corporate websites
- Personal accounts

Methods used by fakers on phishing websites

Fake login forms

Phishing websites often contain login and password forms that look real, but actually send the entered data to scammers.

Imitation of official design

Websites can accurately copy the design of real websites of famous brands, financial organizations or services.

URL manipulation

Fraudsters may use URLs that look very similar to the real ones. To do this, they can change just a few letters *(ffln.kz instead of ffin.kz)* or use a different top-level domain name *(for example,.com instead of .net).*

Fake offers and promotions

Unrealistically profitable offers, high returns or urgent promotions that require immediate entry of personal data.

Malware

Some phishing websites may try to install malicious software on your device under the guise of useful applications.

Hidden redirects

Visiting such a website may silently redirect you to other phishing or malicious websites.

How to recognize phishing websites

1

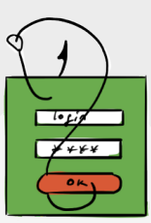
Check the URL.
Fake websites often use URLs that are similar to the real ones, but with slight differences or typos.

2

Availability of HTTPS.
Safe websites use the HTTPS protocol, which ensures protection of transmitted data. Absence of HTTPS may be a sign of phishing.

3

Design and spelling.
Poor design, grammatical and punctuation errors on a website may indicate phishing.



4

Requests for personal information.
Be wary, if a site immediately asks you to enter sensitive data.

How to protect oneself

Do not enter personal information. Official websites of bona fide companies will never request all bank card data, logins and passwords of other services and other personal data.

yes

Use antiviruses with anti-phishing functionality.
They can warn you about visiting suspicious websites.

yes

Two-factor authentication.
Include it, where possible. This way you can further protect your accounts.

yes

Always be cautious and careful, when entering personal information on the Internet.
If you have doubts about authenticity of the website, it is better to reinsure oneself and not enter data.

Don't save passwords in the browser.
Use a reliable password manager.

yes

Update regularly software. Make sure your browser and operating system updated to the latest versions.

yes