FREEDOM
BROKER

КАК НЕ ПОПАСТЬСЯ НА УЛОВКИ МОШЕННИКОВ

FREEDOM BROKER

КАК РАСПОЗНАТЬ ТЕЛЕФОННЫХ МОШЕННИКОВ

и не попасться на их уловки

Как понять, что звонят мошенники

Запрашивают конфиденциальную информацию. Данные банковской карты, информация о финансовых операциях, личные данные, пароли, логины и так далее.

Торопят и создают панику. Действовать нужно немедленно, иначе

Создают искусственную угрозу. Пугают потерей денег, юридическими, финансовыми и кредитными последствиями, которых можно избежать, если выполнить их требования.

Используют сложную терминологию. Ссылаются на несуществующие законы и банковские процедуры, чтобы запутать.

Чем могут воспользоваться мошенники

Неуверенность. Если вы плохо разбираетесь в банковских делах или не уверены, как должны работать сервисы, мошенники могут это использовать.

Желание быстро и легко заработать. Если вам обещают лёгкие деньги, например, большой выигрыш или неожиданный бонус, это может быть ловушкой.

Рассеянность. Если вы заняты или спешите, мошенники могут попытаться вас запутать или заставить совершить необдуманный поступок.

Страх потерять деньги. Если вам говорят, что ваши сбережения в опасности и надо срочно что-то делать, это может быть способом заставить вас действовать без раздумий.

Как защититься от телефонных мошенников

1 **Проверяйте любую информацию.** Если вам звонят от имени банка или другой организации, не спешите выполнять требования. Лучше позвоните по официальному номеру компании, чтобы подтвердить эту информацию.

2 **Не бойтесь отказать.** Уверенно отказывайтесь от любых предложений или требований, если они вызывают сомнения.

3 **Не действуйте под давлением.** Не совершайте никаких операций и не предоставляйте личные данные, если чувствуете давление или панику.

4 **Изучите методы мошенников.** Прочитайте о том, как действуют мошенники, чтобы быть в курсе основных схем мошенничества.

5 **Не предоставляйте конфиденциальную информацию.** Например, пароли или ПИН-коды. Добропорядочные компании и сервисы никогда не будут запрашивать подобную информацию, ведь это противоречит требованиям цифровой безопасности.

6 **Не устанавливайте программное обеспечение или приложения по чьей-либо просьбе.** Особенно если это звонок с неизвестного номера.

FREEDOM BROKER

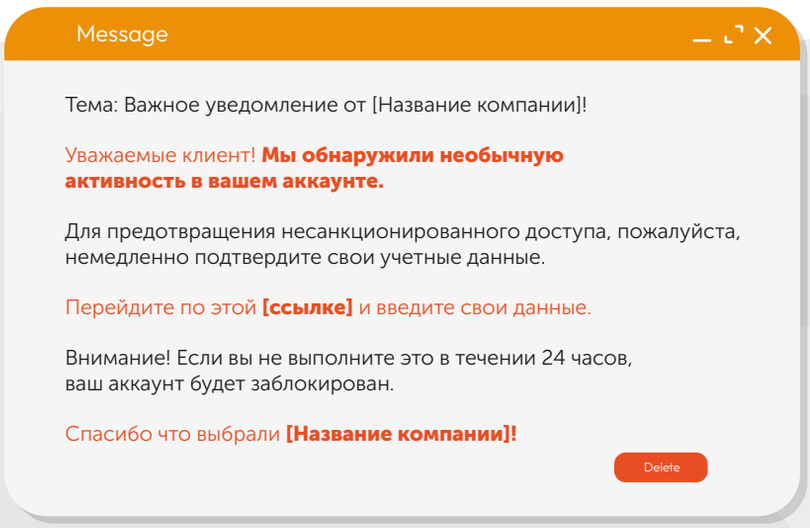
КАК РАСПОЗНАТЬ ФИШИНГОВЫЕ ПИСЬМА и защититься от мошенничества в интернете

Что такое фишинговые письма

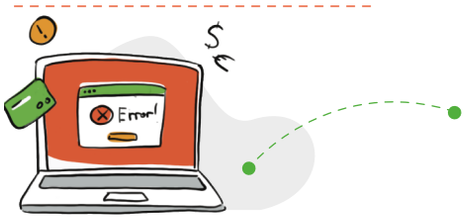
Это ложные сообщения, которые выглядят как официальные письма от финансовых организаций, сервисов или даже ваших друзей. **Цель таких писем — украсть вашу личную информацию** (например, пароли и номера банковских карт).

Как выглядят фишинговые письма

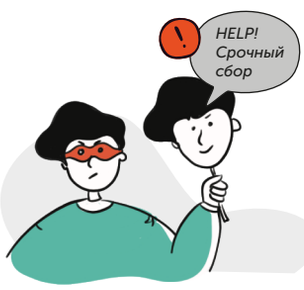
1. Обычно они содержат просьбы срочно что-то подтвердить, изменить пароль или обновить информацию о счете.
2. В письмах могут быть ссылки, ведущие на поддельные сайты, где вас попросят ввести личные данные.
3. Иногда в таких письмах могут быть грамматические ошибки (чтобы обойти спам-фильтры).



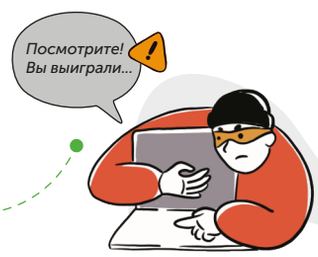
Распространенные схемы мошенничества



Ложные сообщения о блокировке счета. Мошенники утверждают, что ваш счет заблокирован и просят ввести личные данные для его восстановления.



Просьбы о помощи. Мошенники могут притворяться вашими знакомыми и просить перевести деньги, якобы для срочной помощи.



Предложения о выигрыше или наследстве. Вам могут написать о неожиданном выигрыше или наследстве, но для получения придется заплатить или предоставить личные данные.

Как защититься

Не переходите по подозрительным ссылкам. Если вам пришло странное письмо, лучше не кликать по ссылкам внутри него.

yes

Проверяйте адрес отправителя. Если адрес электронной почты выглядит необычно, это может быть фишинговым письмом.

yes

Используйте двухфакторную аутентификацию. Это дополнительный уровень защиты для ваших аккаунтов.

yes

Не делитесь личной информацией. Если не уверены в надежности источника, никогда и нигде не вводите свои пароли, данные карт и другую важную информацию.

yes

Используйте антивирус. Регулярно обновляйте антивирусное программное обеспечение на компьютере.

yes

Будьте внимательны. Если письмо кажется подозрительным, лучше перепроверить информацию, позвонив в финансовую организацию напрямую.

yes

Помните: Всегда лучше перестраховаться и проверить информацию, чем столкнуться с последствиями мошенничества. Будьте бдительны и осторожны при общении в интернете.

FREEDOM BROKER

КАК РАСПОЗНАТЬ ФИШИНГОВЫЕ САЙТЫ

и защититься от них

Что такое фишинговые сайты

Это поддельные веб-страницы, созданные для кражи личных данных (логинов, паролей, номеров банковских карт и другой конфиденциальной информации). Такие сайты могут имитировать популярные страницы и сервисы, чтобы обмануть пользователей и заставить их ввести личные данные.

- Интернет-банкинг
- Социальные сети
- Страницы входа в электронную почту
- Онлайн-магазины
- Торговые платформы
- Корпоративные сайты
- Личные кабинеты

Методы, которые используют мошенники на фишинговых сайтах

Поддельные формы входа.

Фишинговые сайты часто содержат формы для ввода логина и пароля, которые выглядят как настоящие, но на самом деле отправляют введенные данные мошенникам.

Имитация официального дизайна.

Сайты могут точно копировать дизайн настоящих сайтов известных брендов, финансовых организаций или сервисов.

Манипулирование URL-адресами.

Мошенники могут использовать URL, которые очень похожи на настоящие. Для этого они могут изменять всего несколько букв *(ffln.kz вместо ffin.kz)* или использовать другое доменное имя верхнего уровня *(например, .com вместо .net)*.

Фальшивые предложения и акции.

Нереально выгодные предложения, высокая доходность или срочные акции, требующие немедленного ввода личных данных или платежной информации.

Вредоносное ПО.

Некоторые фишинговые сайты могут пытаться установить на ваше устройство вредоносное программное обеспечение под видом полезных приложений.

Скрытые перенаправления.

Посещение такого сайта может незаметно перенаправить вас на другие фишинговые или вредоносные сайты.

Как распознать фишинговые сайты

1

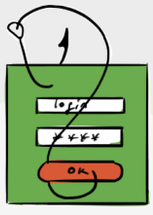
Проверьте URL-адрес.
Поддельные сайты часто используют адреса, похожие на настоящие, но с небольшими отличиями или опечатками.

2

Наличие HTTPS. Безопасные сайты используют HTTPS-протокол, который обеспечивает защиту передаваемых данных. Отсутствие HTTPS может быть признаком фишинга.

3

Дизайн и орфография.
Некачественный дизайн, грамматические и пунктуационные ошибки на сайте могут указывать на фишинг.



4

Запросы личной информации.
Будьте настороже, если сайт сразу же просит ввести конфиденциальные данные.

Как защититься

Не вводите личные данные.
Официальные сайты добросовестных компаний никогда не будут запрашивать все данные банковских карт, логины и пароли других сервисов и другие личные данные.

yes

Используйте антивирусы с функцией защиты от фишинга.
Они могут предупреждать о посещении подозрительных сайтов.

yes

Двухфакторная аутентификация. Включите ее где возможно. Так вы сможете дополнительно защитить ваши аккаунты.

yes

Всегда будьте внимательны и осторожны при вводе личных данных в интернете. Если у вас есть сомнения относительно подлинности сайта, лучше перестраховаться и не вводить данные.

Не сохраняйте пароли в браузере. Используйте надежный менеджер паролей.

yes

Регулярно обновляйте программное обеспечение.
Убедитесь, что ваш браузер и операционная система обновлены до последних версий.

yes