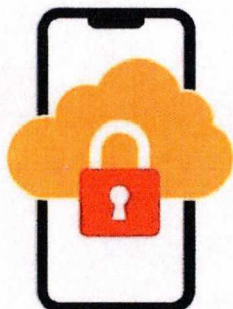


ПОПУЛЯРНЫЕ СХЕМЫ



ФАЛЬШИВЫЕ ОБЪЯВЛЕНИЯ

Мошенники размещают объявления на популярных интернет-площадках, в онлайн-магазинах и социальных сетях. Они предлагают товары по заведомо низкой цене, чтобы выманить у вас предоплату, после чего исчезают.



ОБМАН С ICLOUD

Мошенники предлагают бесплатные игры, высокооплачиваемую работу, затем просят войти в чужой iCloud. После этого телефон блокируют и злоумышленники вымогают деньги за разблокировку.



ЗВОНКИ ОТ «СЛУЖБ»

Мошенники представляются сотрудниками государственных органов, банковских учреждений, а также работниками служб связи и жилищно-коммунального хозяйства. Используя методы психологического давления и запугивания, они стремятся:

- выманить SMS-коды и конфиденциальные банковские данные для доступа к личным кабинетам граждан и хищения денежных средств;
- склонить к переводу личных сбережений на подконтрольные им «безопасные» счета;
- вынудить оформить кредит или передать наличные деньги курьерам.

ВАЖНО ЗНАТЬ



**В нашей стране
не существует
процедуры
декларирования
денежных средств
через перевод их
на безопасный счет
или передачу
третьим лицам.**

5 ПРАВИЛ БЕЗОПАСНОСТИ

1

Используйте безопасные платежи. Не переводите предоплату на личные карты продавцов («по номеру телефона»). При покупках на платформах объявлений пользуйтесь встроенной «Безопасной сделкой», где деньги резервируются системой, а не уходят напрямую продавцу до получения товара.



2

Никому не сообщайте коды из SMS, пароли и личные данные. Не переходите по ссылкам из подозрительных писем и сообщений в мессенджерах.

3

Не входите в чужой iCloud и не передавайте доступ к своему устройству третьим лицам.



4

Не верьте звонкам с угрозами, кем бы ни представился собеседник. Немедленно прекратите разговор!



5

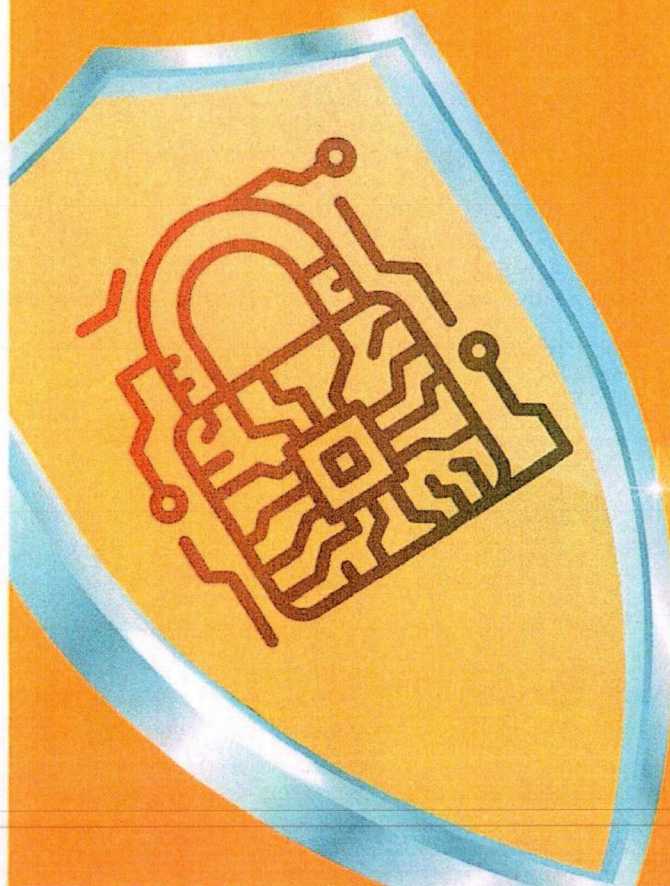
Проверяйте информацию только через официальные контакты организаций.



Если вы подозреваете обман — немедленно обращайтесь в милицию по телефону

102

Соблюдение этих правил и знание того, как действуют мошенники, помогут вам сохранить деньги и спокойствие.



2026

Январь	Февраль	Март	Апрель
Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс
1 2 3 4	1	1	1 2 3 4 5
5 6 7 8 9 10 11	2 3 4 5 6 7 8	2 3 4 5 6 7 8	6 7 8 9 10 11 12
12 13 14 15 16 17 18	9 10 11 12 13 14 15	9 10 11 12 13 14 15	13 14 15 16 17 18 19
19 20 21 22 23 24 25	16 17 18 19 20 21 22	16 17 18 19 20 21 22	20 21 22 23 24 25 26
26 27 28 29 30 31	23 24 25 26 27 28	23 24 25 26 27 28 29 30 31	27 28 29 30
Май	Июнь	Июль	Август
Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс
1 2 3	1 2 3 4 5 6 7	1 2 3 4 5	1 2
4 5 6 7 8 9 10	8 9 10 11 12 13 14	6 7 8 9 10 11 12	3 4 5 6 7 8 9
11 12 13 14 15 16 17	15 16 17 18 19 20 21	13 14 15 16 17 18 19	10 11 12 13 14 15 16
18 19 20 21 22 23 24	22 23 24 25 26 27 28	20 21 22 23 24 25 26	17 18 19 20 21 22 23
25 26 27 28 29 30 31	29 30	27 28 29 30 31	24 25 26 27 28 29 30 31
Сентябрь	Октябрь	Ноябрь	Декабрь
Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс
1 2 3 4 5 6	1 2 3 4	1	1 2 3 4 5 6
7 8 9 10 11 12 13	5 6 7 8 9 10 11	2 3 4 5 6 7 8	7 8 9 10 11 12 13
14 15 16 17 18 19 20	12 13 14 15 16 17 18	9 10 11 12 13 14 15	14 15 16 17 18 19 20
21 22 23 24 25 26 27	19 20 21 22 23 24 25	16 17 18 19 20 21 22	21 22 23 24 25 26 27
28 29 30	26 27 28 29 30 31	23 24 25 26 27 28 29 30	28 29 30 31

2027

Январь	Февраль	Март	Апрель
Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс
1 2 3	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4
4 5 6 7 8 9 10	8 9 10 11 12 13 14	8 9 10 11 12 13 14	5 6 7 8 9 10 11
11 12 13 14 15 16 17	15 16 17 18 19 20 21	15 16 17 18 19 20 21	12 13 14 15 16 17 18
18 19 20 21 22 23 24	22 23 24 25 26 27 28	22 23 24 25 26 27 28	19 20 21 22 23 24 25
25 26 27 28 29 30 31		29 30 31	26 27 28 29 30
Май	Июнь	Июль	Август
Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс
1 2	1 2 3 4 5 6	1 2 3 4	1
3 4 5 6 7 8 9	7 8 9 10 11 12 13	5 6 7 8 9 10 11	2 3 4 5 6 7 8
10 11 12 13 14 15 16	14 15 16 17 18 19 20	12 13 14 15 16 17 18	9 10 11 12 13 14 15
17 18 19 20 21 22 23	21 22 23 24 25 26 27	19 20 21 22 23 24 25	16 17 18 19 20 21 22
24 25 26 27 28 29 30 31	28 29 30	26 27 28 29 30 31	23 24 25 26 27 28 29 30 31
Сентябрь	Октябрь	Ноябрь	Декабрь
Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс
1 2 3 4 5	1 2 3	1 2 3 4 5 6 7	1 2 3 4 5
6 7 8 9 10 11 12	4 5 6 7 8 9 10	8 9 10 11 12 13 14	6 7 8 9 10 11 12
13 14 15 16 17 18 19	11 12 13 14 15 16 17	15 16 17 18 19 20 21	13 14 15 16 17 18 19
20 21 22 23 24 25 26	18 19 20 21 22 23 24	22 23 24 25 26 27 28	20 21 22 23 24 25 26
27 28 29 30	25 26 27 28 29 30 31	29 30	27 28 29 30 31



**Как не
попасться
на удочку
телефонных
мошенников**

**или 5
способов сохранить
сбережения**

ВИШИНГ

НЕ ОТВЕЧАЙ НА ОБМАН!



Вишинг — это вид телефонного мошенничества, при котором злоумышленники выманивают у людей конфиденциальные данные или деньги по телефону.

Они представляются сотрудниками банков, полиции, операторов связи и других организаций, чтобы втереться в доверие и получить доступ к вашим данным.



ПОМНИ:

Звонок от незнакомца — это не всегда важно. Проверяйте информацию, прежде чем доверять или сообщать что-либо. 

КАК РАСПОЗНАТЬ ВИШИНГ?

1



НЕОЖИДАННЫЙ ЗВОНОК

Вам звонят сами, хотя вы никуда не обращались. Мошенники выбирают жертв случайно.

2



ПРЕДСТАВЛЯЮТСЯ СОТРУДНИКАМИ РАЗЛИЧНЫХ СЛУЖБ

Представляют себя сотрудниками банка, милиции, почты и даже поликлиники, чтобы вызвать доверие и оказать давление.

3



ПРОСЬБА СООБЩИТЬ ДАННЫЕ

Просят продиктовать пароли, коды из SMS, данные карт и паспортов или установить приложение.

4



ДАВЛЕНИЕ И СПЕШКА

Говорят, что нужно действовать срочно, иначе будут проблемы, которые повлекут за собой потерю денег.

5



ЦЕЛЬ — ВАШИ ДАННЫЕ И ДЕНЬГИ

Их цель — получить доступ к вашим личным данным и средствам, а также, возможно, похитить вашу информацию или деньги.

КАК ЗАЩИТИТЬСЯ?



ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ

Перезвоните в организацию по официальному номеру, который найдете сами. Не используйте номера из SMS или сообщений.



НЕ СООБЩАЙТЕ ЛИЧНЫЕ ДАННЫЕ

Никому и никогда не сообщайте пароли, коды из SMS и данные карт по телефону.



ПРЕРВИТЕ РАЗГОВОР

Если что-то вызывает сомнение — завершите разговор. Лучше потерять «важный звонок», чем деньги.



НЕ ПОДАВАЙТЕСЬ НА ДАВЛЕНИЕ

Мошенники торопят вас специально, чтобы вы не успели проверить информацию и обдумать действия.



БУДЬТЕ БДИТЕЛЬНЫ

Настоящие сотрудники никогда не запрашивают конфиденциальные данные по телефону.



СТАЛИ ЖЕРТВОЙ ВИШИНГА?

Немедленно смените пароли, заблокируйте карты и обратитесь в банк. Сообщите в милицию по телефону **102**

ФИШИНГ

НЕ КЛЮЙ НА ОБМАН!

Фишинг — это вид интернет-мошенничества, при котором злоумышленники выманивают у людей конфиденциальные данные (пароли, номера карт, логины).

Они маскируются под известные компании, банки или сервисы, чтобы заставить жертву добровольно передать ценную информацию.

ПОМНИ:

Одна ошибка — и ваш аккаунт или деньги в руках мошенников.

КАК РАСПОЗНАТЬ ФИШИНГ?

1



ПОДОЗРИТЕЛЬНЫЕ ССЫЛКИ И ОТПРАВИТЕЛИ

Проверяйте адрес отправителя и ссылки. Даже небольшая ошибка в адресе может быть ловушкой.

2



ЗАПРОС ЛИЧНЫХ ДАННЫХ

Никогда и никому не сообщайте пароли, коды из SMS и данные карты. Настоящие организации этого не требуют.

3



СРОЧНОСТЬ И ДАВЛЕНИЕ

Фразы вроде «срочно», «ваш аккаунт заблокирован» — способ заставить вас потерять бдительность.

4



ОРФОГРАФИЧЕСКИЕ И СТИЛИСТИЧЕСКИЕ ОШИБКИ

Мошенники часто делают ошибки в тексте и оформлении. Будьте внимательны!

КАК ЗАЩИТИТЬСЯ?



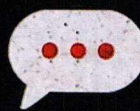
ПРОВЕРЯЙТЕ ИСТОЧНИКИ

Заходите на сайты только через официальные адреса и приложения.



ИСПОЛЬЗУЙТЕ НАДЕЖНЫЕ ПАРОЛИ

Включите двухфакторную аутентификацию везде, где это возможно.



НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ

Не открывайте ссылки из писем и сообщений от неизвестных отправителей.



БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ

Перепроверяйте информацию и не поддавайтесь панике.



СТАЛИ ЖЕРТВОЙ ФИШИНГА?

Немедленно смените пароли, заблокируйте карты и обратитесь в банк. Сообщите в милицию.

**ФИШИНГ
ОПАСНОСТЬ
В ИНТЕРНЕТЕ!**
ВНИМАНИЕ!
МОШЕННИКИ!