

## КАК РАСПОЗНАТЬ ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Если Вам поступил звонок на телефон  
или пришло SMS о том, что:



- Вы выиграли приз
- Нужны деньги, чтобы спасти попавшего в беду родственника
- Вам полагается компенсация
- Ваша банковская карта заблокирована
- Ваш номер будет заблокирован, чтобы этого не произошло, наберите код
- Вам предлагается исцеление по телефону
- В ваш тарифный план внесены изменения, чтобы узнать подробности, отправьте SMS на номер

С осторожностью заполняйте свой профиль в социальных сетях. Не указывайте данные паспорта и адрес проживания.

**В публичном доступе сообщайте о себе минимум информации.**

Если от хорошо знакомого человека пришло сообщение странного содержания, то, возможно, его страницу взломали. В таком случае пытаются вымогать деньги, просят перейти по ссылке или открыть прикрепленный файл. Позвоните человеку, от имени которого пришло подозрительное сообщение. В беседе вы сможете выяснить, отправлял ли он вам такое послание.

Если странное сообщение получено от **незнакомца**, то тем более **не стоит** переходить по ссылкам и открывать файлы. Ссылка может вести на фишинговый мошеннический сайт. А файл может содержать вирусы.

**Заведите отдельную карту для платежей в интернете.**

Если для оплаты в интернете вы пользуетесь своей обычной картой, **не храните** на ней крупные суммы денег.

Вы хотите бесплатно посмотреть или скачать фильм? **Будьте внимательны!** Мошенники создают сайты, на которых надо оставить телефон или отправить сообщение на короткий номер. Так с вашего счета могут списать внушительную сумму за смс, а сам телефон попадет в базу спамеров.

**Приглашаем вас  
в библиотечно-  
информационный центр  
Центральной городской библиотеки!**

**Адрес: г. Ангарск, 17 микрорайон, д. 4**

**Контактный телефон: 8 (3955) 55-09-69**

**Официальный сайт: [cbs-angarsk.ru](http://cbs-angarsk.ru)**

**E-mail: [cbs-angarsk@yandex.ru](mailto:cbs-angarsk@yandex.ru)**

**Составила: Исанбаева Т. В.,  
ведущий библиотекарь ЦГБ**

Муниципальное бюджетное учреждение культуры  
Ангарского городского округа  
«Централизованная библиотечная система»

Отдел «Читальный зал»  
Центральной городской библиотеки

**Безопасность  
пожилых в Интернете**



**Памятка**

**Ангарск  
2021**

Всемирная паутина развивается все быстрее. Это двигатель современного мира, средство оставаться с ним на одной волне.

Но по мере развития интернет-сервисов в сети появляются новые виды мошенничества, причем нацелены они, в первую очередь, на неподготовленных к цифровому миру людей.

Мы надеемся, что простые советы помогут вам, уважаемые пользователи, защититься от мошенников и повысить компьютерную грамотность.

### Советы по безопасности

Вам пришло сообщение о том, что вы миллионный посетитель сайта или выиграли в лотерею. И мошенники просят вас сообщить им ваши личные и банковские данные, чтобы «перевести» выигрыш на ваш счет. Вместо этого ваши сбережения попросту будут украдены.

### Помните:

Используйте **разные пароли** для разных сайтов. Если один пароль действует для многих аккаунтов, под угрозой окажутся все. Если не надеетесь на память, выписывайте данные отдельно и прячьте от посторонних глаз.

- **Вы не можете выиграть в лотерею, если в ней не участвовали.**
- **Никто не раздает деньги просто так.**
- **Никогда не передавайте данные доступа к вашему банковскому счету через Интернет.**

**Не предоставляйте** вашу персональную информацию любому веб-сайту, не задумываясь над тем, зачем он это спрашивает.

Собираясь отправиться в путешествие или другую поездку, не стоит об этом всем заранее сообщать. **Вашим отсутствием могут воспользоваться квартирные воры.** Поделитесь своими впечатлениями и фотографиями после того, как вернетесь домой.

## Правила безопасности в сети Интернет

- Ограничьте объем информации о себе
- Не выкладывайте личную информацию о друзьях
- Не отправляйте свои персональные данные незнакомцам
- Не забывайте выходить из своих аккаунтов
- Заведите себе два адреса электронной почты
- Не пишите грубостей, оскорблений
- Не реагируйте на хамство и грубость других пользователей
- Не используйте Сеть для распространения сплетен, угроз или хулиганства.
- Не оставляйте без присмотра компьютер с важными сведениями на экране
- Используйте только сложные пароли и старайтесь чаще менять их

При подключении к Wi-Fi в общественных местах будьте **внимательны** по отношению ко всему, что вы делаете во время подключения. Выключайте Wi-Fi, когда им не пользуетесь. И себя защитите, и заряд батареи сэкономите. Обязательно **отключите** функцию автоматического подключения к Wi-Fi в вашем телефоне или планшете.

Кэтфишинг - это когда кто-то создает в Интернете **несуществующего** человека и заводит знакомства с людьми с целью **обманом выманить у них деньги**. Они **придумывают** целый сценарий, в котором им нужно будет занять деньги (например, для члена семьи, который заболел, или для полета на самолете, чтобы встретиться с вами).

### Как избежать афер с онлайн-знакомствами

**Не осуществляйте банковские операции. На совершайте покупки. Не входите на почту и в личные профили в соцсетях.**

**Будьте осторожны с теми, кто пытается установить с вами взаимоотношения. Расскажите своим близким о новом знакомстве, чтобы они могли проверить профиль этого человека. Никогда не перечисляйте деньги кому-либо, с кем вы познакомились в Интернете.**

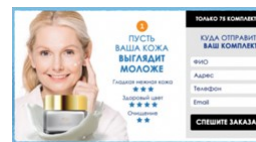
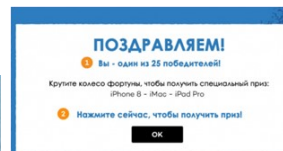
**НЕ ДОВЕРЯЙТЕ** информации, если Вам сообщают, что Ваш родственник или знакомый попал в беду и нужны крупная сумма денег, чтобы «вытащить» его. Это 100% обман!

**НЕ ДОВЕРЯЙТЕ** информации, что у Вас или у Вашего родственника обнаружена опасная болезнь и нужны деньги на лечение или покупку дорогостоящих лекарств – **ВРАЧИ НЕ СООБЩАЮТ**.

**НЕ СОГЛАШАЙТЕСЬ** на приглашения принять участие в розыгрыше призов, купить чудодейственные лекарства, приборы или дешевые вещи и продукты.



**НЕ СОГЛАШАЙТЕСЬ** на предложения снять порчу или сглаз, погадать, предсказать будущее, - это хороший повод завладеть Вашими деньгами.



### Никогда не отвечайте на спам.

Установите и обновляйте антивирусные программы. Устаревшие версии не могут гарантировать защиту от вредоносного ПО. Ежедневно в мире появляется несколько новых вирусов, поэтому антивирусу нужно как можно чаще получать информацию о методах борьбы с ними.

**Не скачивайте сомнительные приложения** и не пытайтесь это делать по неизвестным ссылкам. Пользуйтесь только **официальными** магазинами App Store, Google Play и Windows Market.

