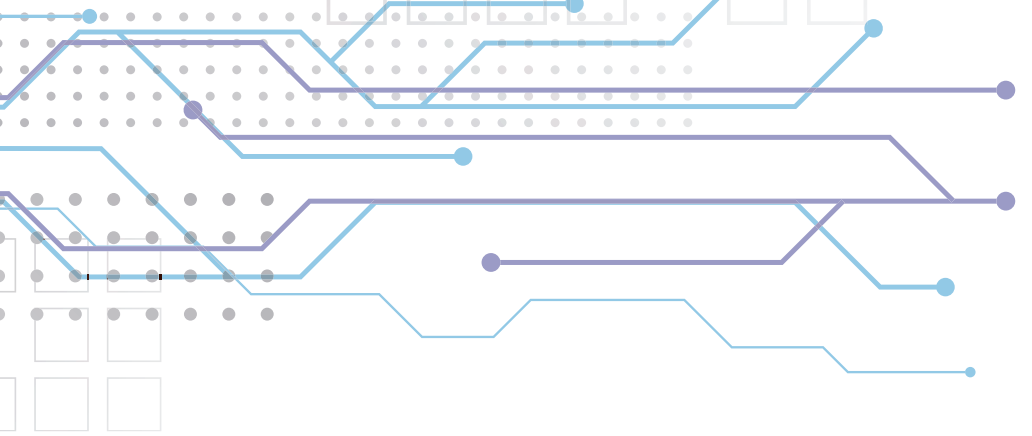
ЦИФРОВАЯ РОССИЯ

Памятка по цифровой безопасности для старшего поколения

Антон Немкин

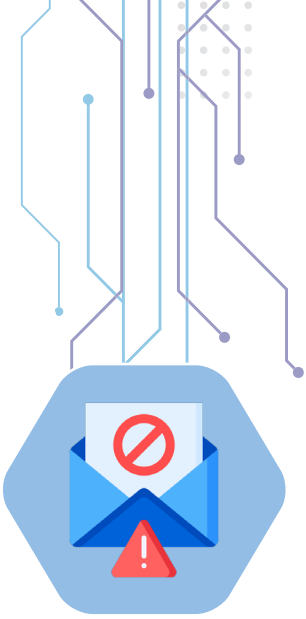
Член комитета Госдумы
по информационной политике,
информационным технологиям
и связи, координатор
федерального партийного
проекта «Цифровая Россия»

В современном мире цифровые технологии пронизывают все сферы жизни. Для пенсионеров и людей старшего возраста развитие навыков цифровой грамотности особенно важно, так как это помогает им получать доступ к важной информации, безопасно пользоваться онлайн-сервисами и при этом избегать встреч с мошенниками. Чем лучше человек понимает, как устроена цифровая среда, тем меньше шансов, что он станет жертвой обмана.



Кроме того, освоение цифровых технологий помогает пожилым людям сохранять социальные связи и активный образ жизни. Они могут общаться с родственниками и друзьями онлайн, записываться к врачу, заказывать товары и даже осваивать новые хобби. При этом обучение цифровой грамотности должно быть доступным и понятным для каждого.

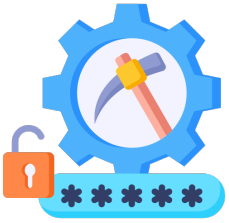
Наш партийный проект «Цифровая Россия» совместно с профильными органами власти и ведущими российскими ИТ-компаниями разработал предложения по формированию комплексной программы и установлению единого стандарта преподавания цифровой грамотности. На основе наших наработок уже сформированы методические материалы, которые помогут всем желающим повысить свою киберграмотность.



Многие пожилые люди верят на слово всем, кто представляется сотрудником государственных организаций: полиции, соцзащиты, поликлиник, банков.

Аферисты пользуются доверчивостью граждан и придумывают схемы, рассчитанные именно на старшее поколение.

Как разоблачить мошенника и не дать себя обмануть?



Мы собрали главные сценарии атак, о которых сегодня должно знать старшее поколение!

«Вам полагается прибавка к пенсии»

Мошенник звонит якобы от имени Социального фонда России (СФР) и сообщает пожилому человеку, что у него есть неучтенный трудовой стаж.
Если подать заявку на перерасчет, можно получить ежемесячную прибавку к пенсии и компенсацию за прошлые годы.

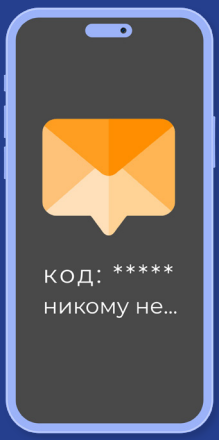
«Сотрудник Соцфонда» уверяет, что для оформления прибавки идти никуда не надо. Достаточно продиктовать реквизиты банковской карты и назвать код, который придет на телефон якобы для подтверждения заявки.

ЗАПОМНИТЬ!

Настоящие сотрудники СФР не обзванивают граждан, чтобы пересчитать пенсию или начислить выплату, и никогда не спрашивают данные карт, особенно – коды из SMS. Они могут запросить документы или уточнить реквизиты для перевода денег, только если вы сами придете в отделение. Если есть сомнение, кто на связи – мошенник или сотрудник СФР – лучше самостоятельно позвонить по номеру круглосуточной горячей линии Соцфонда: **8 800 100-00-01 .**

«Получите новые льготы»

Мошенники сообщают пенсионеру о новых субсидиях или льготах. Чтобы их получить – нужно записаться якобы на прием в МФЦ. Для подтверждения записи просят сверить номер СНИЛС и продиктовать номер электронного талона из SMS.



ЗАПОМНИТЬ!

На самом деле, SMS содержит секретный код. Например, для входа в учетную запись на «Госуслугах». Заполучив доступ к аккаунту человека на госпортале, преступники могут похитить все данные и оформить на его имя онлайн-займы.

«Большие скидки или внезапный выигрыш»

Мошенник сообщает по телефону о специальных ценах и подарках для пожилых или о том, что пенсионер неожиданно выиграл крупную сумму средств, автомобиль или даже квартиру. Для получения спецпредложения, подарка или выигрыша злоумышленник просит продиктовать персональные данные (ФИО, серия, номер паспорта, СНИЛС).

ЗАПОМНИТЬ!

Никогда не сообщайте свои данные по телефону незнакомым лицам, тем более если звонок поступил через мессенджеры – Viber, WhatsApp, Telegram. Не открывайте вложения, фото и видео, которые прислали вам с незнакомого аккаунта. Подобный контент может содержать вредоносные программы, которые передадут все ваши данные мошенникам.

«Ваши деньги в опасности, переведите их на безопасный счет»

Многие пенсионеры откладывают деньги — и за этими накоплениями охотятся мошенники. Часто аферисты предлагают снять их с банковского вклада и внести на «безопасный» счет. Мошенники звонят пенсионерам, представляются службой безопасности банка или сотрудниками силовых структур. Сначала они запугивают пожилого человека – убеждают, что его сбережения находятся под угрозой. Затем подкупают заботой и предлагают решение — перевести все на особый защищенный счет. В реальности этот счет принадлежит мошенникам.

ЗАПОМНИТЬ!

Чтобы не оказаться в такой ситуации, просто не верьте в сказки про «специальные» защищенные счета — их не существует. При этом любой банковский счет будет безопасным, если не выдавать посторонним конфиденциальные сведения.

«Помогаем вернуть деньги, которые вы перевели мошенникам»

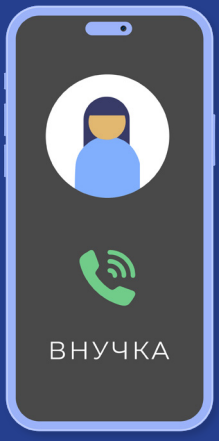
Аферисты часто наживаются на тех, кто уже попался на крючок их сообщников или других преступников. Они находят обманутых людей с помощью рекламы, распространяют объявления, в которых гарантируют возмещение потерь всем, кто перевел деньги мошенникам. Выплатами якобы занимаются некие «Центры компенсаций». Для возмещения убытков на сайтах этих вымышленных организаций, пострадавшие должны оставить данные карт, с которых уходили переводы. Если человек так и поступит, преступники снова украдут его накопления.

ЗАПОМНИТЬ!

Если вы выдали аферистам данные карты или открыли доступ к банковскому личному кабинету, банк не обязан компенсировать потери. Их также не возместят юрфирмы, «Центры компенсаций» или любая другая организация. Не верьте рассказам мошенников и проверяйте существование организаций, от имени которых вам звонят.

«Ваш родственник попал в беду»

На телефон поступает звонок якобы от родственника – ребенка или внука, который попал в опасную ситуацию, и чтобы ему помочь, обязательно нужны деньги. Аферисты просят перевести деньги на банковский счет или сообщить данные своей карты, код из мобильного приложения банка для упрощения перевода.



ЗАПОМНИТЬ!

Обязательно перезвоните родственнику на сотовый и проверьте факты, которые сообщил аферист. Ни в коем случае не сообщайте посторонним лицам данные карты и коды из SMS или приложений банка.

«Подтвердите свои данные для сотового оператора»

Аферист, представившись оператором сотовой связи, сообщает, что срок действия вашей SIM-карты истекает и его необходимо продлить. Мошенники присылают пенсионеру SMS с кодом, который просят сообщить для продления договора. Как только человек передает код, мошенники получают доступ к личному кабинету на «Госуслугах».

ЗАПОМНИТЬ!

Никогда не сообщайте свои данные по телефону незнакомым лицам, тем более если звонок поступил через мессенджеры. Не называйте код, так как сотрудники операторов связи никогда не запрашивают подобные сведения, а действие SIM-карты является бессрочным.

«Срочно оформите кредит»

Человеку звонит «сотрудник бюро кредитных историй» и утверждает, что на него или его близких родственников мошенники пытаются оформить кредит.

Через короткое время ему снова звонят и уже могут представляться сотрудниками «службы безопасности банка», «правоохранительных органов» или «Банка России». Звонящий подтверждает, что на имя пенсионера или его близких неизвестные лица действительно оформляют кредит и, чтобы предотвратить его незаконное оформление, необходимо как можно скорее оформить «встречный» кредит самостоятельно онлайн или в офисе банка. Для убедительности мошенники просят действовать оперативно и ни в коем случае не рассказывать про оформление кредита и его целях кому-либо, так как проводится секретная операция по вычислению жулика из числа сотрудников банка.

ЗАПОМНИТЬ!

Ни сотрудники банков, ни бюро кредитных историй не информируют граждан об изменениях в кредитной истории по телефону. Если вам поступил такой звонок, немедленно положите трубку и ни в коем случае не сообщайте свои персональные данные или данные карт.

«Помогите продавцу маркетплейса»

Мошенник звонит, представляясь продавцом маркетплейса, и просит пенсионера помочь ему поднять свой рейтинг. По словам мошенника, для этого нужно купить его товары. Затем заказ аннулируется и человеку возвращаются деньги, да еще и с благодарностью «продавца» в размере 4-5%. Затем пенсионеру предлагают купить с последующей отменой заказа более дорогой товар. После покупки никакой отмены не происходит, а мошенник больше не выходит на связь.

ЗАПОМНИТЬ!

Не совершайте поспешных действий. Если вас торопят с принятием решения, требуют незамедлительно продиктовать данные, купить товар, перевести деньги, пытаются разжалобить или запугать – немедленно прервите разговор.

«Подтвердите данные для визита в больницу»

Человеку поступает звонок «представителя поликлиники», который сообщает о не пройденной процедуре, на которую якобы была запись. Мошенник угрожает санкциями в виде аннулирования записей и просит срочно подтвердить пройденный анализ (например флюорографию) или другую процедуру, справку, назначение и т.д. Далее жертве предлагают приехать и показать заключение, желательно – прямо сейчас. Если сделать это проблематично, то «заботливый» оператор предлагает пробить пациента по системе. НО! Сделать это невозможно без номера СНИЛС. Как только человек диктует номер СНИЛС, ему приходит код из SMS, который просят назвать. Этот код, как правило, является ключом доступа к вашему аккаунту на «Госуслугах».

ЗАПОМНИТЬ!

Номер СНИЛС является вашим идентификатором на портале «Госуслуги», а последующая SMS открывает доступ к вашему аккаунту, где содержится вся информация о вас - паспорт, трудовая книжка, ПТС на транспорт, счета и другое. Не называйте СНИЛС и код! Сотрудники поликлиники никогда не запрашивают подобные сведения.

«Установите приложение Центробанка»

Злоумышленники звонят гражданам, в том числе через мессенджеры, и утверждают, что неизвестные лица пытаются похитить деньги с их счета. Чтобы предотвратить потерю сбережений, мошенники убеждают человека немедленно установить на своем телефоне якобы мобильное приложение Центрального банка (варианты названий могут быть разными). Причем, пока оно устанавливается, устройством пользоваться запрещают. После этого злоумышленники просят жертву запустить установленное приложение, поднести свою карту к мобильному телефону и ввести подтверждающий SMS-код от банка - якобы для авторизации в приложении и спасения денег на счете. На самом деле загруженная на смартфоне человека программа – это вирус, который позволяет создать на телефоне мошенников виртуальный образ банковской карты жертвы. В результате злоумышленники могут снимать деньги в банкоматах при помощи бесконтактной технологии: вместо банковской карты они прикладывают свой смартфон.

ЗАПОМНИТЬ!

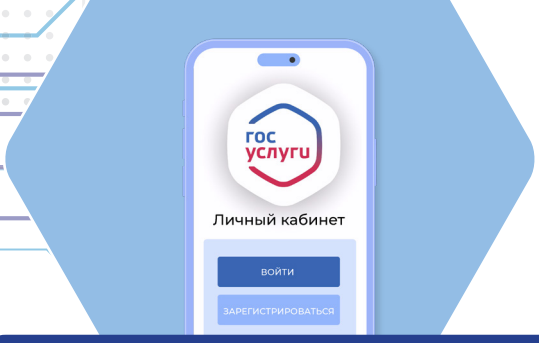
Не скачивайте по просьбе незнакомых лиц никакие мобильные приложения или программы, а также не совершайте по их требованию никаких действий в банковских и иных приложениях. При возникновении любых сомнений относительно сохранности денег на банковском счете сразу же звоните в свой банк по номеру, указанному на его официальном сайте или оборотной стороне банковской карты.

«Поможем найти потерянную посылку»

Мнимые сотрудники «Почты России» звонят вам и предлагают найти потерянную посылку или заказное письмо. Злоумышленники говорят жертве, что нужно уточнить адрес доставки или обновить данные. Они просят перейти в чат-бот Telegram и заполнить форму: добавить трек-номер посылки или письма, ввести свой телефон и авторизоваться через «Госуслуги».

ЗАПОМНИТЬ!

«Почта России» не требует переходить в мессенджеры или чат-боты для подтверждения данных. Если пропали посылка или письмо: зайдите на сайт «Почты России», откройте раздел «Поиск пропавших почтовых отправлений», введите трек-номер и узнайте актуальный статус. Узнать о состоянии отправления можно также в официальном приложении «Почта России». Если у вас есть сомнения, лучше обратиться на горячую линию «Почты России» по номеру 8 (800) 100-00-00 либо уточнить информацию в ближайшем отделении.



ЧТО ДЕЛАТЬ ЕСЛИ АККАУНТ «ГОСУСЛУГИ» ВЗЛОМАЛИ?

ШАГ 1: **Восстановите доступ к учетной записи (например, через электронную почту).**

ШАГ 2: **Защитите аккаунт (смена паролей, двойная защита – двухфакторная аутентификация).**

ШАГ 3: **Определите, где использовалась ваша учётная запись.**

- Перейдите в личный кабинет → Безопасность → Действия в системе. Проверьте, не было ли подозрительных действий в учётной записи. Если были, и учётная запись использовалась на «Госуслугах», обратитесь в службу поддержки. Если на стороннем ресурсе — в службу поддержки данного ресурса.
- Выйдите из приложений, в которые вы не заходили: личный кабинет → Безопасность → Моб. приложения.
- Отзовите разрешения, которые вы не выдавали: личный кабинет → Согласия и доверенности → Разрешения.
- Проверьте поданные заявления. Это поможет выявить, какие действия хотели совершить мошенники от вашего имени.

ШАГ 4: **Подайте заявление в МВД.**

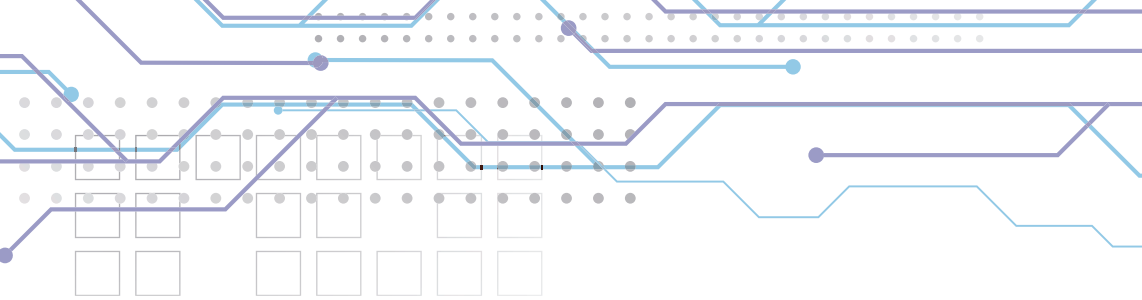
ЧТОБЫ НЕ ПОПАСТЬ НА КРЮЧОК МОШЕННИКОВ:

Не сообщайте коды и личные данные по телефону

Мошенники часто звонят пенсионерам, представляясь сотрудниками банка, полиции или социальных служб. Если вам говорят, что нужно срочно назвать код из SMS, продиктовать паспортные данные или номер карты – это обман. Настоящие организации никогда не запрашивают такую информацию. Если сомневаетесь, повесьте трубку и перезвоните в банк или организацию сами.

Остерегайтесь подозрительных сообщений и ссылок

Если вам пришло сообщение о выигрыше, пенсии, компенсации или блокировке карты, не переходите по ссылкам и не скачивайте вложенные файлы. Лучше позвоните в банк или в Пенсионный фонд и уточните информацию.



Не передавайте деньги «родственникам» без проверки

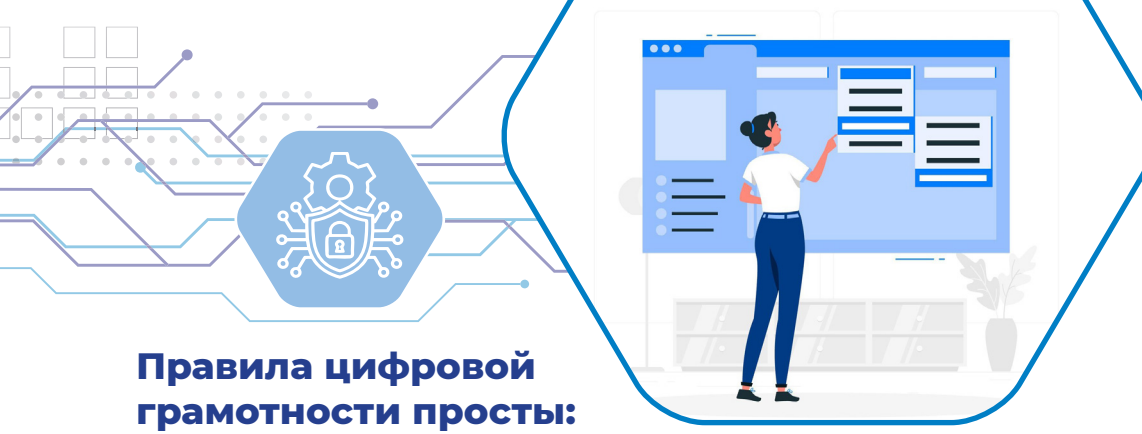
Не спешите отправлять деньги! Позвоните своим родственникам и уточните, действительно ли у них есть проблемы.

Просите помощи у близких

Если вам звонят, пишут или предлагают что-то сделать в интернете, а вы не уверены, безопасно ли это – попросите детей, внуков или соседей проверить информацию. Лучше лишний раз уточнить, чем стать жертвой обмана.

Развивайте навыки цифровой грамотности

Цифровая грамотность — это набор знаний и умений, которые необходимы для безопасного и эффективного использования цифровых технологий, ресурсов интернета и корректной работы с информацией в сети.



Правила цифровой грамотности просты:

1 **Проверяйте подлинность сайта, на котором вас просят ввести свои данные или данные карт.**
Чаще всего мошенники подделывают сайты: «Госуслуги» и другие государственные порталы, сайты банков, страницы оплаты в интернет-магазинах.

ПОМНИМ, что на незнакомых или сомнительных сайтах нельзя вводить свои персональные данные или данные своих банковских карт. Порталы и сайты, которыми часто пользуетесь, лучше поместить во вкладку «избранное».

2 **При поиске информации в интернете проверяйте информацию, которую находите. Не доверяйте фейкам.**
Фейк – это целенаправленно распространяемая ложная информация в интернете, которую специально создают, чтобы запутать, ввести в заблуждение или посеять панику среди граждан.

ПОМНИМ, чтобы не попасться на провокацию, важно искать оригинальный источник новости, откуда она начала распространяться, а также доверять только качественной прессе.

3 **Никогда не предоставляйте ваши персональные данные незнакомым людям.** Персональные данные — это информация о человеке, по которой его можно идентифицировать. Поэтому предоставить свои персональные данные — это все равно, что пустить незнакомого человека к себе домой или отдать ему ключи от квартиры. Зная ваши персональные данные мошенники, могут взять на вас кредит или украсть данные карт и накопительных счетов.

ПОМНИМ, персональные данные в сети помогают сформировать цифровой двойник человека, их нужно охранять.

4 **Игнорируйте спам и сообщения во всплывающих окнах.** Спам – это нежелательные сообщения в любой форме, которые отправляются в большом количестве. Чаще всего спам отправляется в форме коммерческих электронных писем, присланных на большое количество адресов, а также через мгновенные и текстовые сообщения (SMS), социальные медиа или даже голосовую почту. Через такую массовую рассылку приходят не только безобидные рекламные предложения, но и ссылки на вредоносные программы или фишинговые сайты.

ПОМНИМ, не стоит открывать письма от незнакомых адресантов. Внимательно стоит относиться к любым присланным ссылкам – даже если это сообщения от хорошо знакомых вам людей. Их почтой или аккаунтом могли воспользоваться мошенники. Если сомневаетесь, перезвоните отправителю и уточните детали.

5 **Соблюдайте меры осторожности при общении в социальных сетях.**
Социальные сети – это интернет-площадки для общения, обмена информацией и контентом, прочих социальных взаимодействий. Например, «Одноклассники», «ВКонтакте». В социальных сетях не рекомендуется публиковать фотографии, которые потом можно было бы использовать против вас, распространять личные данные. Внимательно относитесь к виртуальным собеседникам, которых вы не знаете лично. Человек может представиться чужим именем, изменить личную информацию о себе, чтобы втереться в доверие или использовать в корыстных целях информацию о вас. Если вы считаете, что общающийся с вами человек вызывает подозрения и ведет себя необычно, лучше прекратите общение с ним.

ПОМНИМ, что, если сделать свои аккаунты в соцсетях закрытыми — это затруднит мошенникам доступ к вашим данным.

6 **Записывайте на бумажных носителях ваши пароли и PIN-коды.** Не храните их в компьютере.
Пароль – это секретная комбинация цифр, букв и других знаков для получения доступа к различным данным или компьютерной программе.
Не используйте в пароле свои имя, фамилию, клички животных, информацию о родственниках. Создавайте пароль из не менее чем 8-10 символов и добавляйте в него строчные и заглавные буквы, цифры и символы. Меняйте пароль хотя бы 1 раз в месяц.

ПОМНИМ, что пароли и PIN-коды не должны дублироваться в разных сервисах.

7 **Пользуйтесь антивирусом.**
Антивирус — это программное обеспечение, состоящее из нескольких слоев защиты и предназначенное для обнаружения, блокировки и удаления вирусов, вредоносных программ, а также для защиты пользователя от других киберугроз.

ПОМНИМ, что актуальное антивирусное программное обеспечение поможет защитить вашу конфиденциальную информацию от мошенников.