Как защититься от мошенников в интернете

Важно уметь не только пользоваться интернетом, но и защищать личную информацию от хакеров и мошенников. Это можно сделать, следуя простым правилам

Правила безопасности в интернете

- Используйте сложные пароли
- Включите двухфакторную аутентификацию для всех своих аккаунтов
- Установите и регулярно обновляйте антивирусное программное обеспечение (ПО) и операционные системы
- Не открывайте подозрительные письма и вложения, не переходите по ссылкам, где требуется ввести личную информацию
- Защитите домашний Wi-Fi паролем
- Не выкладывайте слишком много информации о себе в интернет. Не делитесь ею с сомнительными сайтами
- Рассказывайте о кибербезопасности своим детям и родителям. Научите их быть осторожными в интернете и обсуждать с вами любые сомнительные ситуации

Правила кибербезопасности на работе

- Используйте только одобренные внутренней службой безопасности ресурсы и ПО
- Будьте осторожны при открытии электронных писем — это может быть фишинг
- Не оставляйте рабочие устройства без присмотра и блокируйте их, если отходите
- Храните конфиденциальные данные только на защищённых серверах и устройствах
- Сообщайте обо всех киберинцидентах и нарушениях в отдел информационной безопасности

Как защитить аккаунт на Госуслугах от мошенников

Данные пользователей на Госуслугах надежно защищены. Но иногда мошенники входят в доверие к владельцам профилей и обманом получают от них важную информацию.

Соблюдайте правила безопасности и дополнительно защитите аккаунт удобным способом.

f09f94b9.png Настройте контрольный вопрос

Он поможет восстановить доступ к аккаунту, если забудете пароль. Вопрос может быть любым, ответ должен быть известен только вам. Сделать это можно в личном кабинете.

f09f9189.png Настроить вопрос: clck.ru/akaEX

f09f94b9.png Настройте оповещение на электронную почту

Каждый раз при входе в аккаунт вы будете получать письмо на электронную почту. Если в аккаунт входите не вы, сообщите об этом через платформу обратной связи: clck.ru/akaFJ

f09f94b9.png Включите вход с подтверждением по смс

При входе в аккаунт вы каждый раз будете получать смс. Для доступа нужно ввести код из сообщения.

f09f94b9.png Никому не сообщайте код из смс

Сотрудники Госуслуг никогда не будут просить назвать код, потому что это конфиденциальная информация, только для вас.

Как обманывают мошенники

Сейчас мошенники выбирают для своих действий тему QR-кода как наиболее актуальную. Например, звонят или пишут с просьбой сообщить сведения, связанные с аккаунтом Госуслуг под предлогом проверки кода. Но темы могут быть разными, а правила безопасности всегда одни.

СЭД МВД
№1157 от 17.01.2023

Инструктаж по профилактике мошеннических действий, совершенных посредством Интернет-технологий, банковских карт, смс-рассылки и мобильного банка.

Во избежание мошеннических действий в отношении лица, необходимо следовать следующим правилам:

- **не сообщать** третьим лицам номера счетов, банковских карт и их реквизиты, логины и пароли от личных кабинетов, коды подтверждения операций, указанные в поступающих смс-сообщениях;

- перед тем как осуществить операции по переводу денежных средств неизвестному лицу, представившемуся родственником, другом, знакомым, попавшим в трудную ситуацию, связаться с ним иным способом для подтверждения его просьбы;

- если сообщили, что банковская карта заблокирована или по счету банковской карты происходят операции по переводу денежных средств, обратиться в отделение банка, в котором обслуживается банковский счет или по номеру телефона службы поддержки, указанному на оборотной стороне банковской карты, не **выполнять указания лица, представившего сотрудником банка**;

- не использовать мобильный телефон с подключенной услугой «Мобильный банк» для выхода в интернет без установленных антивирусных программ, не переходить по **неизвестным ссылкам,** указанным в рекламных сообщениях, так как при этом на телефон может быть загружено вирусное программное обеспечение, в результате чего может произойти списание денежных средств со счета банковской карты;

- **не перечислять денежные средства** при совершении покупок в интернет-магазинах или иных интернет-сайтах, приложениях и социальных сетях («Авито», «Вконтакте». «Одноклассники»), **не убедившись в благонадежности контрагента.** Внимательно изучать рейтинг контрагента на доске объявлений, почитать отзывы других покупателей, поискать информацию о нем в сети «Интернет»;

- **не пользоваться услугами непроверенных и неизвестных сайтов** по продаже билетов, путевок, бронирования отелей и т.д. Обращать внимание на электронные адреса сайтов известных компаний и агентств, так как имеются сайты-клоны, со схожими адресами, зачастую отличающимися одним символом, используемые для мошеннических действий;

- **не размещать в открытом доступе и не передавать посторонним лицам информацию личного характера.** Информация, может быть сохранена злоумышленниками и впоследствии использована в противоправных целях.

- **не перечислять денежные средства** под предлогом активации выигрышей в различных рекламных акциях, лотереях, розыгрышах и т.д.;

- **для перечисления** денежных средств на счет банковской карты, достаточно знать только ее номер, не сообщать никому другой дополнительной информации и не подключать услугу «Мобильный банк» к иному номеру.

Одним из наиболее актуальных вопросов является защита прав граждан от незаконного получения доступа к их персональным данным, электронной цифровой подписи (далее - ЭЦП). Доступ посторонних лиц к указанным сведениям, в том числе в личном кабинете на сайте «Госуслуги», может повлечь совершение мошенничеств в отношении денежных средств и имущества гражданина, а также совершение от имени гражданина иных противоправных действий.

Гражданам не следует относиться к сайту «Госуслуги», как к информационному сайту и компрометировать логин и пароль доступа к нему (утрачивать или передавать третьим лицам).

В настоящее время данный сайт предоставляет возможность пользоваться большим перечнем услуг и данный перечень продолжает расширяться.

Например, может совершаться целый рад операций с недвижимым имуществом гражданина (получение выписок из ЕГРН, постановка на кадастровый учет недвижимости и регистрация права (в определенных случаях), внесение сведений или исправление ошибок в ЕГРН, установление или снятие запрета на сделки с недвижимостью, установление сервитута и др.). В настоящее время Минцифры и Росреестр ведут работу по дальнейшей цифровизации сделок с недвижимостью.

Таким образом, злоумышленник, завладев доступом к личному кабинету гражданина, может, используя его электронную цифровую подпись, совершать от имени гражданина юридически значимые действия, в том числе совершить преступление в отношении самого гражданина, либо действуя от имени гражданина, совершить преступления в отношении третьих лиц, а также интересов общества и государства.

Через сайт «Госуслуги» возможно моментальное получение доступа к вашим личным кабинетам на сайтах других федеральных органов. Так, на сайте ФНС России содержатся данные о счетах гражданина во всех банках, сведения о его движимом и недвижимом имуществе, о наличии задолженности по налогам, а также имеется возможность распоряжения денежными средствами налогоплательщика, возвращенными ему налоговым органом (переплата по налогам, налоговые вычеты).

На сайте «Госуслуг» могут содержаться ранее загруженные гражданином персональные данные родственников, а также сканы и

фотографии важных документов, ранее направлявшихся в государственные органы. Используя копии данных документов мошенники, могут, даже без получения в последующем доступа к личному кабинету гражданина, оформить на его имя получение кредита или нескольких кредитов в разных кредитных учреждениях либо совершить иные незаконные сделки.

Одним из основных способов завладения паролем доступа к личному кабинету является звонок гражданину с предложением изменить пароль доступа к личному кабинету, в связи с истечением срока его действия или по иной причине, а также пройти дополнительную аутентификацию. При этом злоумышленник просит сообщить ему необходимые данные для дистанционного доступа с другого устройства (компьютера, смартфона и т.д.) к личному кабинету гражданина. После получения доступа к личному кабинету гражданина указанные лица могут предпринять действия для получения электронной цифровой подписи для совершения дальнейших неправомерных действий.

Гражданину не следует соглашаться на подобные предложения, сообщать кому бы то ни было свои персональные данные и пароль доступа к личному кабинету.

До недавнего времени вход на сайт «Госуслуг» был возможен через ввод логина и пароля. По информации Минцифры РФ с 1 июня 2023 года, в связи с необходимостью повышения защиты персональных прав граждан и защиты от мошенничеств, вводится двухфакторная аутентификация, что снижает возможность неправомерного доступа к личному кабинету гражданина.

Дополнительная авторизация осуществляется путем направления СМС с одноразовым кодом на номер телефона, ввода одноразового кода через приложение, с использованием биометрических данных. Настройка доступа к личному кабинету производится на сайте «Госуслуг» (gosuslugi.ru), где также содержатся подробные инструкции по подключению двухфакторной аутентификации и использованию цифровых сервисов, связанных с использованием ЭЦП.

Тем не менее, доступ злоумышленников к персональным данным может быть возможен в случае передачи посторонним лицам поступающих на телефон СМС с паролями доступа.

Таким образом, в условиях продолжающейся цифровой трансформации общества, граждане, в целях защиты от мошенничеств, должны крайне

внимательно относиться к хранению и использованию паролей доступа к сайту «Госуслуги», цифровой подписи и усиленной квалифицированной электронной подписи, а также файлов и носителей их содержащих. При возникновении любых сомнений в компрометации паролей, совершении через личный кабинет действий посторонними лицами следует принять меры к блокировке доступа в личный кабинет и незамедлительно обратиться в органы внутренних дел.

Осторожно! Мошенники!

В условиях развития цифровой экономики, электронных платежных систем персональных электронных устройств и Интернета стремительно выросло количество совершенных с их использованием преступлений. Такие преступления происходят по нескольким причинам: доверчивость граждан, недостаточная их осведомленность и пренебрежительное отношение к элементарным правилам безопасности.

Наиболее часто используемыми схемами совершения мошенничества являются:

- телефонные звонки от имени работников банковских и кредитных организаций или сотрудников правоохранительных органов;

- представителей инвестиционных компаний и брокерских фирм;

- получение конфиденциальных сведений по банковским картам при покупке (продаже) товаров с использованием сайтов объявлений;

- площадок маркетплейсов;

- используется старая схема «Ваш родственник попал в ДТП» или в больницу.

Также постоянно появляются новые схемы мошенничества:

- Телефонные мошенники стали представляться по-новому. Теперь они якобы почтальоны.

В этом году зарегистрирован первый факт мошенничества, совершенного под видом сотрудника "Почты России".

49-летнему Василию (имя изменено), работающему оператором роботизированных станков крупного предприятия г. Уфы, позвонил неизвестный и, представившись работником "Почты России", сообщил, что якобы на имя Василия из "налоговой" адресовано письмо. Лжепочтальон предложил это письмо доставить в МФЦ и убедил Василия назвать код из смс-сообщения, чтобы "в МФЦ это письмо приняли". На самом деле потерпевшему на мобильный телефон поступил код для восстановления доступа к учётной записи на портале "Госуслуг", которым воспользовались мошенники.

В дальнейшем по известной схеме Василию позвонили лжесотрудники "Госуслуг", "Центробанка" и "МВД". Обещая обезопасить банковские счета, они убедили Василия снять со своих счетов 842 тысячи рублей наличными и внести их через банкомат на "безопасные" счета мошенников.

Запомните, код из смс-сообщения равносилен вашей собственноручной подписи, а самый безопасный счёт - это ваш счёт, открытый именно вами в отделении банка, а не какой-то другой, названный вам неизвестным лицом!

Также в последнее время в полицию поступает все больше обращений от людей, которых злоумышленники лишили накоплений, спекулируя на теме СВО. Они убеждают неравнодушных граждан жертвовать на нужды участников спецоперации, но деньги, как правило, оседают в карманах мошенников.

Будьте внимательны. Если вам позвонил сотрудник банка, то обратите внимание:

Сотрудники банка по телефону или в электронном письме не запрашивают:

- персональные сведения (серия и номер паспорта, адрес регистрации, имя и фамилию владельца карты);

- реквизиты, срок действия, ПИН- и CVV-коды банковских карт;

- пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;

- логин и пароль для входа в личный кабинет клиента банка.

Сотрудники банка также не предлагают:

- установить программы удаленного доступа (или иные сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов);

- перейти по ссылке из СМС-сообщения;

- включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк;

- под их руководством перевести для сохранности денежные средства на «защищённые» или «безопасные» счёта;

- зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

Банк может инициировать общение с клиентом только для консультаций по предоставляемым услугам. При этом звонки совершаются с номеров, указанных на оборотной стороне карты, на официальных сайтах и банковских документах. Иные номера не имеют никакого отношения к банку.

Чтобы не стать жертвой дистанционного мошенничества следует использовать только официальные каналы связи:

- формы обратной связи на сайте банка и в мобильном приложении;

- телефоны горячих линий;

- группы или чат-боты в мессенджерах (если таковые имеются).

Важно помнить, что мобильные приложения банков следует скачивать через официальные магазины (App Store, Google Play и т.п.).

Жертвами мошенников становятся не только граждане преклонного возраста, но и молодые люди, которые в течение нескольких дней заключают кредитные договоры с банковскими структурами, перечисляя баснословные суммы преступникам.

Как обезопасить личные данные?

- не доверять телефону как средству коммуникации;

- не предоставлять в телефонных звонках никакой информации;

- не совершать действий, которые связаны с финансами и конфиденциальными сведениями;

- не пытаться по возможности перейти от коммуникации по телефону к личному общению;

- не реагировать на SMS без подписи с незнакомых номеров;

- внимательно относиться к звонкам с незнакомых номеров.

Обо всех фактах мошенничества необходимо незамедлительно сообщить сотрудникам полиции по номерам:- "02" с городского, "102" с мобильного или обратиться в ближайший отдел полиции.

Будьте бдительны, не доверяйте незнакомцам, не становитесь жертвами мошенников!