

бо все оо

Федеральной  
15.06.2022 г.  
Н.М.  
ДП

# ОТДЕЛ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ И ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ АДМИНИСТРАЦИИ СУСУМАНСКОГО ГОРОДСКОГО ОКРУГА

686314 Магаданская обл., г. Сусуман, ул. Советская, 17. Телеграф: Сусуман, Магаданской, Сусуманского.  
Телефон (41345)-2-25-16, 9148525633, e-mail: OvsyannikovPP@49gov.ru

От .06.2022 № 116

Руководителю Комитета по образованию  
администрации Сусуманского ГО  
Шатуновой Е.А.

Уважаемая Елена Александровна!

В целях информирования населения Сусуманского городского округа об актуальных видах хищений денежных средств с использованием информационно-телекоммуникационных технологий, а также способах и средствах защиты от подобных преступных посягательств, прошу разместить на сайтах организаций культуры и спорта следующую информацию:

**Отдел по делам гражданской обороны и чрезвычайным ситуациям  
администрации Сусуманского городского округа!**

## **ВНИМАНИЕ! МОШЕННИКИ!**

Для оформления документов, исполнения банковских операций по платежам, управления вкладами сейчас широко используются онлайн-сервисы. Но развитие технологий способствует активизации аферистов в Интернете. Обманывать доверчивых граждан в Сети гораздо проще. Киберпреступники придумывают все новые виды и схемы обмана.

Существует несколько наиболее распространенных видов мошенничества:

- **«Фишинг** — кража идентификационных данных (например, ФИО, пароль и номер банковской карты). Преступники выдают себя за надежный источник в сети, вынуждая жертву передать им личные данные.
- **«Кардинг** — тип интернет-преступлений, при котором мошенники обманом путем совершают кражу конфиденциальной информации о пользователях и снимают деньги со счетов граждан без их ведома.

Самые распространенные схемы мошеннических действий в киберпространстве:

686314, г. Сусуман  
Комитет по образованию  
Вх.№ 1371  
15.06.2022

- **Двойники интернет-магазинов.** Невероятно дешевые товары и горячие предложения за полцены призваны завлечь ничего не подозревающих онлайн-покупателей.
- **Копии сервисов интернет-банкинга.** Посредством электронного письма или смс мошенники приглашают пользователей пройти авторизацию. Невнимательные граждане переходят на фальшивый сайт, регистрируются в личном кабинете, раскрывая логин и пароль для доступа к финансам. Мошенники при получении данных опустошают банковские счета.
- **Фишинговая атака по электронной почте.** Рассылка писем с сообщением о выигранном призе или о блокировке счета. Преступники, как правило, просят победителя перевести определенную сумму для получения крупного выигрыша или внести оплату для разблокировки карты.
- **Взлом аккаунтов и рассылка от друзей с целью наживы.** Мошенники пишут на почту или в соцсети родственникам и знакомым владельца страницы с просьбой срочно перевести деньги, придумывая различные ситуации.
- **Фальшивые сайты благотворительности, туроператоров или авиакомпаний.** Необходимость срочно собрать деньги на лечение больного ребенка или слишком низкие цены на путевки, просьбы перевести деньги на заграничный банковский счет или электронный кошелек, — все эти моменты насторожить пользователей.
- **Предложения выгодного заработка.** Недобросовестные работодатели предлагают удаленную работу. Но предварительно требуют оплатить организационные нужды. Как только человек переводит деньги, выдуманная организация исчезает.

В последнее время мошенники часто представляются сотрудниками службы безопасности банков или правоохранительных органов. Звонящий сообщает о попытке взлома или блокировки банковской карты, подозрительных действиях в интернет-банке, пропущенном платеже по кредиту или угрозе штрафа по надуманному обвинению. На самом деле сотрудники служб безопасности банков никогда не звонят клиентам, а о подозрительной деятельности или других проблемах сообщают другими способами.

Получив звонок от незнакомого человека, обратите внимание на то, что и как он хочет вам сообщить. Мошенники стремятся теми или иными способами надавить на жертв — торопить, запутывать, угрожать возможными последствиями. В такой ситуации важно сохранять спокойствие. Даже если вам угрожают потерей всех денег на счетах, не спешите выполнять требования звонящего.

Также мошенник может несколько раз подряд задавать жертве вопросы, на которые можно ответить только словом «да». Столкнувшись с такими вопросами, старайтесь давать другие ответы, переспрашивать или переводить разговор на другую тему.

Если вам звонят «из банка» — попробуйте задать уточняющие вопросы, например, о состоянии счета или последних операциях по карте. Скорее всего, злоумышленник ничего не сможет ответить. Если вам предлагают какую-либо выплату — уточните основание, на котором она производится.

Мошенники стремятся получить секретные данные карты — трёхзначный код CVC/CVV с обратной стороны, коды подтверждения из SMS, логины и пароли от интернет-банков. Настоящие сотрудники банка никогда не запрашивают эту информацию — для обеспечения безопасности они используют отдельные технические средства. Для отправки платежа нужен только номер карты — другие данные для этого не нужны.

Аферисты преследуют единственную цель — обманным путем получить деньги или имущество. Среди них есть психологи, специалисты по финансам, экономике, страхованию и т.д. Они умеют располагать к себе, играть на эмоциях и чувствах.

**Будьте внимательны! Не дайте себя обмануть!**

И.о. начальника отдела по делам ГО и ЧС  
администрации Сусуманского ГО



А.В. Федоров

*Исп. Занина Ю.Д.  
2-23-22*