



ПРОКУРАТУРА
Российской Федерации

ПРОКУРАТУРА
Иркутской области
Нижнеудинская
межрайонная прокуратура
ул. 2-я Пролетарская, 18
г. Нижнеудинск, 665106



Главам муниципальных образований по
прилагаемому списку

08.09.2023 № Исорг-20250046-1576-23/-20250046

Во исполнение п. 3.6 Регламента исполнения приказа Генерального прокурора РФ от 02.08.2018 № 471 «Об организации в органах прокуратуры работы по правовому просвещению и правовому информированию населения, утверждённого приказом Генерального прокурора Иркутской области от 19.10.2018 № 128, направляю Вам для размещения на сайте администрации муниципального образования буклет: «Виды и схемы интернет-мошенничества».

Приложение: на 2 л.

Заместитель прокурора

советник юстиции

М.В. Митрофанова

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 7848BC672715B39B54CD66C8C5CB8CD4

Владелец **Митрофанова Мария Владимировна**

Действителен с 03.03.2023 по 26.05.2024

А.В. Грылева
, 8(914) 881-76-76

Нижнеудинская межрайонная прокуратура
Иркутской области

№ Исорг-20250046-1576-23/-20250046

КУДА СООБЩАТЬ О МОШЕННИЧЕСТВЕ В ИНТЕРНЕТЕ:



в службу технической поддержки банка или платежной системы, осуществляющей переводы денежных средств, чтобы заблокировать счет;

в полицию по месту проживания;

в Роскомнадзор, осуществляющий контроль за деятельностью организаций по оказанию услуг в области электронных технологий.



**ЕСЛИ У МОШЕННИКОВ
ЕСТЬ ВРЕДОНОСНЫЙ
САЙТ, ТО СООБЩИТЬ О
НЕМ ДЛЯ ОПЕРАТИВНОЙ
БЛОКИРОВКИ МОЖНО В
СЛУЖБУ ПОДДЕРЖКИ
БРАУЗЕРА (ЯНДЕКС,
ГУГЛ ИЛИ Т. П.).
ПРИ ПРЕДОСТАВЛЕНИИ
УБЕДИТЕЛЬНЫХ
ДОКАЗАТЕЛЬСТВ САЙТ
ЗАБЛОКИРУЮТ.**



**ВИДЫ И СХЕМЫ
ИНТЕРНЕТ-
МОШЕННИЧЕСТВА**

**НИЖНЕУДИНСКАЯ
МЕЖРАЙОННАЯ
ПРОКУРАТУРА
РАЗЪЯСНЯЕТ**



**ПРЕСТУПНИКАМИ
ЕЖЕДНЕВНО СОЗДАЮТСЯ
НОВЫЕ СХЕМЫ ОБМАНА В
ИНТЕРНЕТЕ. БЕЗОПАСНОСТЬ
В КИБЕРПРОСТРАНСТВЕ ВО
МНОГОМ ЗАВИСИТ ОТ НАС
САМИХ. ПОЭТОМУ СЛЕДУЕТ
БЫТЬ ВНИМАТЕЛЬНЕЕ И
ПРИМЕНЯТЬ НЕКОТОРЫЕ
ПРАВИЛА.**

ИНТЕРНЕТ-МОШЕННИЧЕСТВО -

это вид киберпреступности, заключающийся в хищении чужого имущества или приобретении права на чужое имущество путем обмана или злоупотребления доверием с использованием сети “Интернет”, что является преступлением в соответствии со ст. 159 УК РФ.

ПОПУЛЯРНЫЕ ВИДЫ ИНТЕРНЕТ- МОШЕННИЧЕСТВА:

✓ ФИШИНГ -

кража идентификационных данных (например, ФИО, пароль и номер банковской карты). Злоумышленники пользуются невнимательностью граждан и закупают конфиденциальной информацией путем создания сайтов-клонов, фальшивых аккаунтов в мессенджерах и соцсетях, электронной рассылки писем. Преступники выдают себя за надежный источник в сети, вынуждая жертву передать им личные данные.

✓ КАРДИНГ -

тип интернет-преступлений, при котором мошенники обманным путем совершают кражу конфиденциальной информации о пользователях и снимают деньги со счетов граждан без их ведома. Самый распространенный способ получения доступа к данным банковских карт — взлом серверов интернет-магазинов, расчетных и платежных систем. Хакеры используют программы удаленного доступа и вредоносное ПО (программное обеспечение) для получения персональной информации о человеке и данных о платежной карте.

РАСПРОСТРАНЕННЫЕ СХЕМЫ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ В КИБЕРПРОСТРАНСТВЕ:

ДВОЙНИКИ ИНТЕРНЕТ- МАГАЗИНОВ

Пользователи переходят по ссылке и вводят информацию о своем банковском счете для завершения покупки. В итоге продавец получает оплату и пропадает или присылает совершенно иной товар. Нужно всегда проверять адресную строку в браузере. Она должна начинаться с "https" (безопасный протокол передачи данных).

КОПИИ СЕРВИСОВ ИНТЕРНЕТ- БАНКИНГА

Злоумышленники создают сайты-клоны банков. Посредством электронного письма или смс-сообщения приглашают пользователей пройти авторизацию. Граждане переходят на фальшивый сайт, регистрируются в личном кабинете, раскрывая логин и пароль для доступа к финансам.

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.

