



Прокуратура Российской Федерации
Прокуратура Пермского края

**Прокуратура
Уинского района**

ул. Свободы, 27, с. Уинское
Пермский край, Россия, 617520
тел. (34259) 2-34-35

25.01.2021 № 6-1-2021

Главе администрации Уинского
муниципального района

Зелёнкину А.Н.

Уважаемый Алексей Николаевич!

В целях предупреждения хищения денежных средств при использовании банковских карт, прошу разместить соответствующие разъяснительные материалы на официальном сайте администрации Уинского муниципального округа в информационно-телекоммуникационной сети «Интернет», информационных стендах администрации Уинского муниципального округа.

О результатах необходимо сообщить в прокуратуру района с приложением соответствующих материалов.

Приложение: памятка «О мерах по предупреждению хищения денежных средств при использовании банковских карт».

Прокурор района
младший советник юстиции

И.В. Суетин

Е.И.Булатова, 2-34-80



Рекомендуется:

При возникновении
малейших подозрений насчет
предпринимаемых попыток
совершения мошеннических
действий следует
незамедлительно уведомить
банк.

Уважаемые жители Уинского муниципального округа!
О противоправных действиях при использовании банковских карт Вы можете
сообщить в:

- **ОМВД России по Уинскому муниципальному округу** по адресу: с. Уинское,
ул. Свободы, 27. Тел.: (834259) 2-34-54

- **Прокуратуру Уинского района** по адресу: с. Уинское, ул. Свободы, 27.
Тел.: (834259) 2-34-35



Прокуратура Уинского района

**О мерах по
предупреждению
хищения
денежных средств
при
использовании
банковских карт**

с. Уинское, 2021

Для предотвращения противоправных действий по снятию денежных средств с банковского счета необходимо исходить из следующего:

- сотрудники банка не запрашивают персональные сведения, реквизиты и сроки действия карты, пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены, логины и CVV код банковской карты;
- сотрудники банка не предлагают установить программы удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов с устройства);
- сотрудники банка не предлагают перейти по ссылке из СМС-сообщения или включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк;
- сотрудники банка не предлагают под их руководством перевести для сохранения денежных средств на «защищенный счет» или зайти в онлайн-кабинет по ссылке из СМС-сообщений.

При использовании мобильного телефона соблюдайте следующие правила:

- при установке приложений обращайтесь внимание на полномочия, которые они запрашивают. Будьте особенно осторожны, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и доступ к сети «Интернет»;
- отключайте в настройках возможность использования голосового управления при заблокированном экране;
- следует использовать только надежные официальные каналы связи с кредитно-финансовыми учреждениями. В частности, форму обратной связи на сайте банка, онлайн-приложения, телефоны горячей линии, группы или чат-боты в мессенджерах, а также официальные банковские приложения из магазинов App Store, Google Play, Microsoft Store.

Необходимо соблюдать меры по обеспечению конфиденциальности реквизитов карты, в том числе:

- подключение к общедоступным сетям Wi-Fi;
- использование ПИН-кода или CVV-кода при заказе товаров и услуг через сеть «Интернет», а также по телефону;
- сообщения кодов третьих лицам (в противном случае любые операции, совершенные с использованием ПИН-кода или CVV-кода, считаются выполненными самим держателем карты и не могут быть опротестованы);
- отдавайте предпочтение банкоматам, установленным в защищенных местах (например, в госучреждениях, банках, крупных торговых центрах)