**СОВЕТЫ ПО ЗАЩИТЕ ОТ ИНТЕРНЕТ-МОШЕННИЧЕСТВА:**

1. Будьте внимательны при предоставлении личной информации.

2. Остерегайтесь подозрительных ссылок и вложений в электронных письмах.

3. Используйте надежные пароли.

4. Будьте осторожны при совершении онлайн-покупок.

5. Не раскрывайте свои банковские данные и коды доступа.

6. Устанавливайте надежное антивирусное программное обеспечение.

7. Внимательно читайте условия и политику конфиденциальности.

8. Используйте защищенное подключение к Wi-Fi.

9. Будьте внимательны и осторожны при общении в социальных сетях.

10. Будьте внимательны во время онлайн-игр и конкурсов.

**НАКАЗАНИЕ ЗА МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ**

Ответственность за мошенничество (в том числе за мошенничество в интернете) предусмотрена ст. 159 УК РФ. Санкция этой статьи по ч. 1 устанавливает следующие виды наказаний:

* штраф в размере до 120 тыс. руб.;
* штраф в размере зарплаты или иного дохода осужденного, полученного им за период, не превышающий одного года;
* обязательные работы продолжительностью до 360 часов;
* исправительные работы продолжительностью до 1 года;
* ограничение свободы / принудительные работы продолжительностью до 2 лет;
* арест продолжительностью до 4 месяцев;
* лишение свободы продолжительностью до 2 лет.



Прокуратура
Кильмезского района
Кировской области

ПРОКУРАТУРА

Кильмезского района

Кировской области



**МОШЕННИЧЕСТВО:
ЧТО ЭТО И КАК С НИМ БОРОТЬСЯ?**



пгт. Кильмезь

2025 год



**МОШЕННИЧЕСТВО** – это преступление, совершаемое при помощи обмана и злоупотребления доверием. Злоумышленники изучают психологию и используют человеческие слабости. Жажда легкой наживы и чрезмерная доверчивость – вот два основных свойства человеческой натуры, которые используются при совершении мошенничества.

**ВИДЫ МОШЕННИЧЕСТВА.**

* **Фишинг** — это метод мошенничества, при котором злоумышленник пытается получить личную информацию, такую как пароли, номера кредитных карт и другие данные, представляясь легитимным и доверенным источником. Это может происходить через фальшивые веб-сайты, электронные письма или сообщения.
* **Вишинг** — это один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определенных действий со своим карточным счетом / платежной картой.
* **Фарминг** — это процедура скрытного перенаправления жертвы на ложный IP-адрес. Для этого может использоваться навигационная структура.
* **Кликфрод** — один из видов сетевого мошенничества, представляющий собой обманные клики на рекламную ссылку лицом, не заинтересованным в рекламном объявлении.
* **«Нигерийские письма»**— вид мошенничества, получивший наибольшее развитие с появлением массовых рассылок по электронной почте. Как правило, мошенники просят у получателя письма помощи в денежных операциях, обещая солидные проценты с сумм.

Если получатель согласится участвовать, у него постепенно выманиваются все более крупные суммы денег якобы на оформление сделок, уплату сборов, взятки чиновникам, и т. п.

* **Спам** — это нежелательные и неприглашенные сообщения, которые могут содержать вирусы, рекламу, ссылки на фальшивые веб-сайты или предложения о мошеннических схемах. Спам может поступать по электронной почте, в социальных сетях, на форумах и других платформах.
* **Мошеннические интернет-магазины -** мошенники могут создавать поддельные веб-сайты с предложениями по продаже товаров или услуг. Они могут использовать фальшивые фотографии, описания и предложения с низкими ценами для привлечения покупателей. После получения платежа мошенники не отправляют товар или предоставляют услугу низкого качества.