Памятка по цифровой безопасности и правовой грамотности

Внимание! Эта памятка поможет вам разобраться в основных киберугрозах и предостережёт от действий, которые могут привести к серьёзной уголовной ответственности. Знание этих правил — ваша защита в цифровом мире.

Часть 1: Осторожно, финансы! (Статья 187 УК РФ)

Что запрещено?
Статья 187 УК РФ преследует **неправомерный оборот средств платежей**. Это означает, что под запретом:

- **Изготовление, покупка, хранение или продажа** поддельных банковских карт, платёжных поручений или иных платёжных документов.
- **Создание, приобретение или передача** специальных устройств, компьютерных программ или электронных носителей информации, **цель которых** — незаконный приём, выдача или перевод денежных средств (например, программы для взлома онлайн-касс, устройства для клонирования карт).

Что это значит для вас на практике? Простые примеры рисков:

- **Продажа или покупка банковской карты/счёта** на сомнительных сайтах или у незнакомцев («аренда счёта для бизнеса»). Даже если вам обещают, что это «легально», такие карты почти всегда используются для отмывания денег, полученных преступным путём.
- **Передача своих банковских реквизитов (карты, электронного кошелька)** другому лицу для получения и перевода денег за вознаграждение («обналичивание»). Закон считает это **неправомерной операцией**, так как вы используете своё средство платежа не для своих целей, а для манипуляций с чужими, часто незаконными, средствами.
- **Участие в схемах** с переводом денег через ваш счёт с последующим выводом («дроп»). Это классический состав преступления.

Чем грозит нарушение?

- Лишение свободы на срок **до 6 лет** (а если действовала организованная группа — **до 7 лет**) со штрафом.

- Важно: Эта статья является **тяжким преступлением**, что влечёт суровые последствия для судимости.

Часть 2: Опасные технологии и данные (Новые статьи 274.3, 274.4, 274.5 УК РФ)

С 1 сентября 2025 года вступили в силу новые статьи, направленные на борьбу с современными киберпреступлениями. Они касаются оборудования и данных, используемых для анонимных или мошеннических действий в сети.

1. Статья 274.3: Незаконное использование специального телефонного оборудования

- **Что запрещено?** Незаконное использование или обеспечение работы так называемых **GSM-гейтов (абонентских терминалов пропуска трафика)** или виртуальных АТС. Это оборудование часто используется мошенниками для массовых звонков, спама и скрытия своего реального номера.
- **Чем грозит?** Даже простое использование такого оборудования с целью совершить другое деяния (например, мошенничество) грозит **лишением свободы до 2 лет**.
- **2. Статья 274.4: Нелегальная торговля мобильными номерами**
- **Что запрещено?** Организация или участие в деятельности по **незаконной передаче (продаже) абонентских номеров** другим лицам. Часто это делается для регистрации аккаунтов на чужие паспортные данные.
- **Простой пример:** Заплатить деньги, чтобы получить для регистрации в мессенджере или соцсети сим-карту, оформленную на другого человека. Участие в такой схеме — это состав преступления.

3. Статья 274.5: Торговля доступом к аккаунтам

- **Что запрещено?** Организация или участие в сборе и продаже **данных для авторизации** (логины, пароли, одноразовые коды) к любым интернет-ресурсам (соцсети, почта, банки).
- **Простой пример:** Покупка или продажа «взломанных» аккаунтов в социальных сетях или игровых сервисах. Даже если вы не взламывали их сами, а лишь участвуете в их перепродаже, вы нарушаете закон.

Чем грозит нарушение статей 274.4 и 274.5?

- За **участие** в такой деятельности — штраф до 300 тыс. рублей или **лишение свободы до 2 лет**.
- За **организацию** — наказание строже: штраф до 700 тыс. рублей или **лишение свободы до 3 лет**.
-

Часть 3: Золотые правила цифровой гигиены

Следуя этим простым правилам, вы защитите себя не только от мошенников, но и от невольного нарушения закона.

1. **Ваши данные — только ваши.** Никогда и никому не передавайте свои банковские карты, реквизиты доступа к онлайн-банку, паспортные данные, логины и пароли. Не продавайте и не «давайте в аренду» свой номер телефона, аккаунты в соцсетях или мессенджерах.
2. **Не участвуйте в сомнительных схемах.** Если вам предлагают «лёгкий заработок», связанный с переводом денег через ваш счёт, регистрацией фирм, аккаунтов или получением посылок — это 99% мошенничество или отмывание денег. Ваши действия могут быть квалифицированы как соучастие.
3. **Остерегайтесь подозрительных устройств и программ.** Не приобретайте и не используйте «волшебные» USB-ключи, SIM-боксы, программы для взлома или автоматизации действий в интернете. Их назначение часто является противоправным.
4. **Проверяйте информацию.** Получили предложение о работе или услуге? Проверьте компанию, почитайте отзывы.
5. **Двухфакторная аутентификация — ваш друг.** Всегда включайте её для важных сервисов (почта, банк, соцсети). Это значительно усложнит злоумышленникам доступ к вашим аккаунтам, даже если они узнают пароль.

Помните: Незнание закона не освобождает от ответственности. В цифровом мире ваши действия оставляют след, и правоохранительные органы могут установить причастность к противоправной деятельности. Будьте бдительны и законопослушны!