

Что делать, если вы стали жертвой?

- Немедленная блокировка. Если заметили подозрительные списания — заблокируйте карту. В некоторых случаях каждая минута может иметь значение, так как мошенники могут моментально вывести средства.

- Обращение в банк. Позвоните на горячую линию, сообщите о факте мошенничества, оформите письменное заявление. Банки часто рекомендуют дополнительные меры, например смену логина в мобильном приложении.

- Заявление в полицию. Предоставьте скриншоты, распечатки, свидетельства телефонных разговоров. Чем раньше вы заявите, тем выше шансы вернуть средства или хотя бы признать вас официально потерпевшим. Не стоит затягивать с этим, иначе расследование может осложниться.

- Смена паролей. Если мог быть скомпрометирован ваш аккаунт в соцсетях или почте, оперативно меняйте все пароли. Лучше перестраховаться и заменить комбинации на всех критически важных ресурсах.

Куда обращаться за юридической и психологической помощью?

- Полиция. Они занимаются расследованием цифровых преступлений, могут запросить логи, IP-адреса, связаться с банками.

- Банки (службы безопасности, горячие линии). Если проблема связана с финансовыми операциями, банк — ваш первый союзник в попытке вернуть средства или заблокировать мошеннические переводы.

- Общественные организации (правозащитные центры, кибердружины, «горячие линии» по интернет-безопасности). Такие организации консультируют граждан, помогают грамотно составить заявление, в некоторых случаях обеспечивают бесплатную юридическую поддержку.

- Психологические службы (государственные и частные) — при необходимости работы с травмой или профилактики повторного вовлечения. Иногда стресс от обмана или угроз может сильно сказаться на эмоциональном состоянии, и профессиональная помощь окажется незаменимой.

ГБОУ СО «Североуральская школа-интернат, реализующая адаптированные основные общеобразовательные программы»



Алгоритмы действий при возникновении «Цифровых проблем»

**Г. Североуральск
2025 год.**

Если вовлечен ребёнок: пошаговое руководство для родителей

1. Сохраняйте спокойствие: обвинения и крики только усилят скрытность подростка. Поняв, что «его отругают», он может начать удалять переписки и уничтожать важные доказательства.

2. Соберите факты: какие аккаунты, куда переводились деньги, с кем велась переписка. Создайте копии переписки, сделайте скриншоты, чтобы при необходимости предоставить их в полицию.

3. Блокируйте опасные каналы: заморозьте или удалите сомнительные аккаунты, карты, SIM-карты. Лучше перестраховаться и свести потенциальный ущерб к минимуму, чем потом расхлёбывать последствия.

Если вовлечен ребёнок: пошаговое руководство для родителей

4. Обратитесь за юридической консультацией: чем раньше вы действуете, тем больше шансов избежать серьёзных правовых последствий.

Иногда своевременное обращение может повлиять на исход дела, если докажете, что вы сами стали жертвой обмана и вовремя сообщили об этом.

5. Работайте с психологом (при необходимости), чтобы помочь ребёнку пережить стресс и осознать свой поступок. Юридический аспект — важен, но и эмоциональная сторона не менее значима, особенно если подросток чувствует вину и боится дальнейших шагов.

Как понять, что ваши счета и аккаунты использовались незаконно?

- Необычные транзакции: приход крупных сумм от незнакомых людей, мгновенный вывод на другие счета, отсутствие внятного объяснения. Если ребёнок или кто-то из семьи не может ясно пояснить, откуда эти деньги, следует провести разбирательство.

- Подозрительные SMS или push-уведомления о переводах, которых вы не совершали. Иногда банк может заблокировать операцию или прислать уведомление, что происходит «подозрительная активность».

- Изменения в настройках интернет-банка: привязка новых номеров или email, неизвестные шаблоны платежей. Если вы никогда не устанавливали такие параметры, возможна компрометация.

- Внезапная блокировка банковского аккаунта по требованию службы безопасности. Это знак, что банк уже заподозрил что-то неладное, и вам нужно как можно скорее связаться с его представителями.