Кибермошенничество — **это один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путём хищения личной информации пользователя** (номеров банковских счетов, паспортных данных, кодов, паролей и так далее).

Основные цели кибермошенничества:

* хищение уникальных, ценных данных для последующего использования, перепродажи;
* изменение или полное удаление данных с целью необходимос

Мошенничество в интернете — популярнейший вид преступлений в мире. Злоумышленники отличаются от классических грабителей и воришек высоким интеллектом и цифровой грамотностью. Поймать их нелегко, ещё сложнее посадить. Законодательная база часто не поспевает за изобретательностью сетевых злоумышленников. Только вы способны позаботиться о своих финансах и приватной информации. Для этого достаточно выполнять несколько правил кибергигиены.

Содержание:

* [Киберпреступность — что это такое?](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C)
  + [Рождение хакеров: феномен киберпреступности](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%A0%D0%BE%D0%B6%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5)
  + [На кого охотятся киберпреступники?](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%9D%D0%B0)
* [Что и как крадут киберпреступники?](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%A7%D1%82%D0%BE)
  + [Личные данные пользователя в преступных схемах](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%9B%D0%B8%D1%87%D0%BD%D1%8B%D0%B5)
  + [Шантаж с использованием личных данных](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%A8%D0%B0%D0%BD%D1%82%D0%B0%D0%B6)
  + [Кража данных финансовых карт](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%9A%D1%80%D0%B0%D0%B6%D0%B0)
* [Способы кибермошенничества](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%A1%D0%BF%D0%BE%D1%81%D0%BE%D0%B1%D1%8B)
* [Что говорит закон: какое наказание за киберпреступления в РФ?](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%A7%D1%82%D0%BE2)
* [Признаки, что вас хотят «развести»: на что обращать внимание?](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%9F%D1%80%D0%B8%D0%B7%D0%BD%D0%B0%D0%BA%D0%B8)
* [Я стал жертвой кибермошенничества — что делать?](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%AF)
* [Основы кибербезопасности](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D1%8B)
  + [Защита номера](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%97%D0%B0%D1%89%D0%B8%D1%82%D0%B0)
  + [Защита банковских данных](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%97%D0%B0%D1%89%D0%B8%D1%82%D0%B02)
  + [Защита аккаунтов](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%97%D0%B0%D1%89%D0%B8%D1%82%D0%B03)
* [Защита детей от мошенников](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%97%D0%B0%D1%89%D0%B8%D1%82%D0%B04)
* [Итоговый чек-лист](https://gdemoideti.ru/blog/ru/kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov#%D0%98%D1%82%D0%BE%D0%B3%D0%BE%D0%B2%D1%8B%D0%B9)

Киберпреступность — что это такое?



Prostock-studio/Shutterstock.com

Исследователи этого многогранного явления определяют киберпреступность как **любое противозаконное деяние, нарушающее права и свободы человека с помощью компьютерных систем и сетей**. Спам-рассылка — минимум, на что способны преступники.

Киберпреступления совершаются ради всем понятной цели — обогащение. Только на 2021 год показатели совершения подобных нарушений [выросли](https://gdemoideti.ru/blog/exit.php?url=https://tass.ru/obschestvo/10616343?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com) в 11 раз. Одно из 4 самых частых преступлений — это кибермошенничество. Хакеры не скупятся на самые хитрые способы добычи сведений:

* номеров банковских карт;
* личной информации;
* паролей от почты и различных аккаунтов.

С такой добычей злоумышленники могут поступить несколькими способами:

1. Увести ваши средства.
2. Похитить рабочие данные.
3. Прибегнуть к шантажу, используя приватные фото или переписки.

**Рождение хакеров: феномен киберпреступности**



Prostock-studio/Shutterstock.com

Первая крупная волна киберпреступлений произошла в 80 годах — массовая e-mail рассылка. Люди открывали электронные письма с вредоносным ПО, и преступники получали доступ к данным пользователей для своих корыстных целей. Такой способ мошенники используют по сей день.

В 90-е развитие веб-браузеров породило новые методы киберпреступлений: вирусные программы попадали на компьютеры не подозревающих людей после посещения сомнительных сайтов.

Развитие социальных сетей в 2000-е стало плодородной почвой и для развития кибермошенничества. У злоумышленников появились новые способы для добычи личной информации: возможности доступа к банковским счетам для разнообразных финансовых афер. Сегодня киберпреступность носит мировые масштабы.

**На кого охотятся киберпреступники?**



Prostock-studio/Shutterstock.com

Профессиональные хакеры охотятся за крупной добычей — их жертвами становятся:

* корпорации;
* состоятельные организации;
* торговые сети;
* сайты электронной коммерции и пр.

Мошенники с менее продвинутыми навыками преследуют обычных граждан, у которых есть чем поживиться. Конечно, в зону риска чаще попадают более состоятельные люди. Те, у кого финансовый счёт не превышает 50 тысяч рублей, не такая лакомая добыча для хакеров, однако и они не застрахованы от посягательств злоумышленников на их данные.

Наиболее часто жертвами кибермошенников становятся пенсионеры, пожилые люди — более доверчивы и менее разбирающиеся в технологиях.

Что и как крадут киберпреступники?



Prostock-studio/Shutterstock.com

Пока развивался интернет, мошенники оттачивали методы добычи информации для своих корыстных целей. Данные — это главный объект охоты для киберпреступников. Масштаб последствий зависит от типа данных, которые удалось похитить.

**Личные данные пользователя в преступных схемах**

Любой пользователь оставляет информационный след. Мошенники получают информацию не только из социальных сетей, но и по номеру телефона, и ФИО. Имея только эту информацию, можно узнать, что и когда вы продавали, каким имуществом владеете, какой у вас автомобиль.

В некоторых случаях мошенники, получая доступ к паспортным данным, СНИЛС и другим документам, делали человека номинальным директором для отмывания миллионных сумм. А фиктивный руководитель нёс полную юридическую ответственность. Бывали и такие случаи: по постам в Instagram преступники выясняли, когда хозяева уезжают в отпуск. Их опустевшая квартира становилась объектом кражи или чёрных риэлторских сделок.

**Шантаж с использованием личных данных**

Наверняка вы сталкивались со взломом страницы вашего знакомого в социальной сети, когда мошенники от его имени просят занять денег. Ещё злоумышленники иногда используют данные против самого владельца: например, угрожают выложить личные фото или опубликовать переписку, что нанесёт ущерб репутации жертвы. В этом случае вымогатели требуют круглую сумму за нераспространение приватных данных в интернет. Также существует кибершантаж — требование денег для прекращения кибератаки.

**Кража данных финансовых карт**

Банки тратят немало усилий и средств, чтобы защитить деньги клиента. Но часто данные попадают к мошенникам из-за невнимательности самих пользователей. Например, владелец карты называет номер пластика неизвестным, которые представились работниками банка по телефону. Некоторые пользователи оставляют данные карты на сомнительных ресурсах, совершая транзакцию, или хранят пароль от карты на компьютере в папке «пароли», доступ к которому хакер может получить с помощью вредоносного ПО.

Способы кибермошенничества



Prostock-studio/Shutterstock.com

Вы можете открыть письмо от неизвестного отправителя и загрузить вирус на компьютер, который удалит или повредит ваши файлы. Мошенники также могут украсть важную рабочую информацию из файлов.

Злоумышленники способны получить доступ к вашей странице в социальных сетях. Это значит, что они не только могут писать вашим друзьям, но и получат доступ ко всем вашим перепискам: сообщениям, фото, документам, которые вы когда-либо отправляли.

Старайтесь не отвечать на звонки с незнакомых номеров: мошенники часто представляются работниками банка. Они манипулируют, чтобы вызвать тревогу, говорят, что с вашего счёта пытаются вывести деньги и вам нужно срочно назвать номер карты, чтобы это остановить.

**Методы кибермошенничества**

|  |  |
| --- | --- |
| **Вредоносное ПО** | Вирусные программы, которые нарушают работу системы, собирают данные, копируют или уничтожают файлы. |
| **Форд** | Получение данных банковской карты после оплаты пользователем покупки на вредоносном сайте. |
| **Фишинг** | Сообщения и электронные письма с вредоносным ПО. |
| **Кибератака через посредника (MitM)** | Распространённый вид мошенничества в интернете. Перехват данных во время переписки или обмена информацией между двумя устройствами. |
| **0-day «уязвимость нулевого дня»** | Когда хакеры могут атаковать уязвимости, которые разработчик ещё не обнаружил и не защитил. |
| **DDoS-атака «Отказ в обслуживании»** | На сайт или сервер поступает непрерывный поток ложных запросов. В результате ресурс перестаёт работать из-за перегрузки. |
| **Атака на DNS-сервер (с английского дословно «система доменных имен»)** | Мошенничество в сети, которое применяется зачастую для получения информации о доменах: IP-адреса устройства, маршрутизации почты и пр. |

⠀

Что говорит закон: какое наказание за киберпреступления в РФ?



Prostock-studio/Shutterstock.com

С правовой точки зрения, киберпреступлением считается любое нарушение закона с использованием компьютера или других цифровых устройств. Мошенники готовы не только писать вам письма и сообщения в мессенджерах, но и названивать по телефону, чтобы «выпытать» нужную информацию.

[Европейская конвенция по киберпреступности](https://gdemoideti.ru/blog/exit.php?url=https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185) относит к киберпреступлениям не только незаконный перехват и кражу данных, а также компрометацию компьютерных сетей, но и:

1. нарушение авторских прав;
2. незаконные азартные игры;
3. продажу запрещённых предметов и домогательство.

Одним словом, всё, что может нанести не только финансовый, но и репутационный ущерб.

В России действует три статьи[УК РФ: 272, 273, 274](https://gdemoideti.ru/blog/exit.php?url=http://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/). Вкратце: те, кто неправомерно получил доступ к компьютерной информации и распространяет вредоносные программы, преследуются по закону. Также срок грозит тем, кто нарушает правила хранения, обработки и передачи компьютерной информации. Представление о киберпреступности в России во многом совпадает с положениями европейской конвенции.

Размер штрафа и срок наказания зависит от тяжести преступления. Максимально злоумышленникам может грозить свыше миллиона штрафа и срок до семи лет по ст. 272. В соответствии со ст. 273 — ограничение свободы до четырёх лет и лишение права занимать определённые должности в течение трёх лет. По ст. 274 грозит до пяти лет лишения свободы.

Государство обязывает компании защищать персональные данные, чтобы они не попали к злоумышленникам. Крупные киберпреступные группировки, ворующие миллионы, иногда попадаются сотрудникам ФСБ.

Однако часто злоумышленники, работающие по-мелкому, остаются безнаказанными, потому что их трудно вычислить: вернуть деньги почти невозможно. Даже восстановить справедливость затруднительно. Представители правоохранительных органов, в первую очередь, призывают граждан сохранять бдительность и не вовлекаться в мошеннические схемы.

Признаки, что вас хотят «развести»: на что обращать внимание?



Prostock-studio/Shutterstock.com

Стоит повысить бдительность, когда во время общения с незнакомцем, будь то переписка или телефонный разговор, вам что-то очень активно предлагают, рассказывают о ваших проблемах и, самое главное, призывают к немедленным действиям. Если вас торопят перевести деньги, назвать номер счёта или иного документа, что-то куда-то отправить, открыть какую-то ссылку, и при этом нужно сделать это срочно, то остановитесь и задумайтесь. Перепроверка информации занимает от нескольких минут до нескольких секунд.

Если вам сообщили, что проблемы у близкого человека, перезвоните ему и уточните. Если якобы сотрудники службы безопасности какой-либо организации говорят, что проблемы у вас, перезвоните в организацию. Если вам пишет друг, говоря, что у него проблема: перезвоните ему и уточните — возможно, его взломали.

Также обращайте внимание на подозрительные сайты. Особенно, если на странице вас призывают к активному и решительному действию. Иногда это может быть маркетинговый ход, но особенно стоит насторожиться, если у вас требуют деньги, а перевод предлагают выполнить через всплывающее окно.

Я стал жертвой кибермошенничества — что делать?



Prostock-studio/Shutterstock.com

Если вы всё-таки стали жертвой кибермошенников и недосчитались на своём счету круглой суммы, то сохраняйте спокойствие. Необходимо выяснить, что именно произошло. Возможно, вы обнаружили, что у вас списали деньги с карты. Не исключено, что вы отправили средства «липовому» интернет-магазину. Или у вас выманили кругленькую сумму через переписку в соцсетях или во время телефонного разговора.

Что бы ни случилось, важно сохранить всю информацию. Сделайте скриншоты переписок, сайта фальшивого магазина, номера счёта, куда были отправлены средства, сохраните телефон, с которого вам звонили. Это будет служить и доказательством и зацепкой, что в отношении вас совершено противоправное действие. Далее действовать нужно через банк и полицию. Следуйте инструкции:

1. Свяжитесь с банком и попробуйте отменить операцию.
2. Заблокируйте возможности операций со счетами и картами.
3. Запросите детализацию в банке с расчётного счета. Если средства ушли в другой банк, напишите заявление о приостановке платежа и возврате средств.
4. Напишите заявление в полицию о хищении денежных средств. Также потребуется выписка из банка для подтверждения и детализация расходов.

Самое главное — предотвратить дальнейшую утечку средств. Есть небольшой шанс, что удастся вернуть похищенные деньги. Если мошенничество совершено через социальные сети, то свяжитесь с администрацией и передайте всю информацию о злоумышленнике. Также поменяйте пароль на более надёжный. Но наиболее надежный способ — это превентивные меры по кибербезопасности. Соблюдение простых инструкций убережёт вас от новых мошенников.

Основы кибербезопасности



Prostock-studio/Shutterstock.com

Защиты требуют все сведения: и банковские аккаунты, и социальные сети. Чем меньше информации о вас в открытых источниках, тем сложнее использовать её против вас. Если доступ мошенникам будет затруднён, то они с меньшей инициативой захотят тратить время и силы на добычу ваших данных.

1. Всегда храните пароли в защищённом месте, не пользуйтесь автосохранением.
2. Кроме того, эксперты рекомендуют периодически менять пароли и чистить сookies — временные интернет-файлы, которые хранят информацию о посещённых страницах (логины, пароли, историю заказов) и позволяют отследить вашу активность.
3. Проверяйте надёжность ресурса и интернет-магазинов, которые вы посещаете.
4. Установите блокировщик рекламы. Так вы защитите себя не только от навязчивых сообщений, но и помешаете установке программ, с помощью которых злоумышленники пытаются получить доступ к вашим файлам.

**Защита номера**



Prostock-studio/Shutterstock.com

Большинство аккаунтов привязаны к вашему номеру, поэтому стоит позаботиться о его защите. Также необходимо обезопасить от атак свой смартфон.

|  |  |
| --- | --- |
| **Защита телефона** | Установите пин-код или графический ключ на смартфон. Не используйте дату рождения свою или близких, чтобы было трудно подобрать пароль в случае кражи или утери. |
| **Пин-код на сим-карту** | Не ленитесь установить пин-код на сим-карту. Если телефон попадёт в руки мошенников, то они не смогут воспользоваться вашим номером, когда карта будет запаролена. |
| **Запрет на действия с сим-картой** | Оформите его в офисе мобильного оператора на случай, если злоумышленники сделают дубликат по поддельной доверенности. |
| **Определитель номера** | Злоумышленники звонят часто с номеров, которые помечаются как мошеннические. |
| **Установка антивируса на смартфон** | Это поможет минимизировать угрозу вредоносного ПО. Платные антивирусные программы более надежны. |
| **Обновление ПО** | Это позволяет защититься от новых способов хакерских атак. Разработчики «латают» в новой оболочке слабые места. |
| **Кодовое слово для сим-карты** | Установите его в офисе мобильного оператора. Так вы быстро заблокируете её после потери или кражи. |

⠀

**Защита банковских данных**



Prostock-studio/Shutterstock.com

Защита информации о банковских счетах и картах — наиболее простой способ уберечь себя от кражи средств. Не распространяйте данные карты, держите в секрете cvv-код — три цифры на обратной стороне пластика. И старайтесь проверять звонки «якобы от банка».

|  |  |
| --- | --- |
| **Храните данные в секрете** | Никому не сообщайте. Особенно неизвестным, которые представляются работниками банков. |
| **Уточняйте официальную информацию** | Самостоятельно перезванивайте на официальные банковские номера, чтобы уточнить информацию. |
| **Уведомления через push, а не sms** | Push — наиболее надёжный протокол, его сложнее отследить, чем уведомления по sms. |
| **Запрет на «Мобильные переводы»** | В офисе мобильного оператора оформите запрет на мобильные переводы средств. Иначе деньги могут снять в случае утери телефона или сим-карты. |
| **Запомните кодовые слова** | Это поможет быстро подтвердить вашу личность в банковском колл-центре. |
| **Подключите оповещения** | Оповещения по дебетовой и кредитной карте помогут отследить все операции. |
| **Безопасные операции** | Оплачиваете онлайн-покупки только на проверенных сайтах. Не вводите данные во всплывающих окнах, где нет информации о платёжной системе. |

⠀

**Защита аккаунтов**



Prostock-studio/Shutterstock.com

Третий пункт — защита почтовых аккаунтов, профилей в социальных сетях и личных кабинетов на сайтах. Не отвечайте на сообщения от неизвестных и не переходите по ссылкам от незнакомых источников. Старайтесь не оставлять личную информацию на сторонних ресурсах.

|  |  |
| --- | --- |
| **Надёжные пароли** | Создавайте пароли, которые сложно разгадать. Не используйте даты рождения, избегайте одинаковых паролей на разных сайтах. |
| **Защита паролей** | Старайтесь хранить пароли в памяти или записывайте в блокнот, который никто не найдёт. Не сохраняйте пароли в папках на телефоне или компьютере. |
| **Отключите автосохранение паролей** | Пароли хранятся в браузере. Если есть доступ к вашему компьютеру или телефону, можно узнать пароль почти от любого сайта, если включена функция автосохранения. |
| **Закройте аккаунт** | Открытые аккаунты в социальных сетях — это полный доступ к личной информации для злоумышленников: где вы живёте, на чём ездите, где отдыхаете. Сделайте соцсети доступными только для друзей. |

⠀  
Установка антивируса на персональный компьютер также необходима. Стоит установить надёжный пароль для WI-FI роутера. Не посещайте личные страницы через общественные сети, старайтесь пользоваться мобильным интернетом. Эти нехитрые правила помогут защитить данные от мошенников.

Защита детей от мошенников



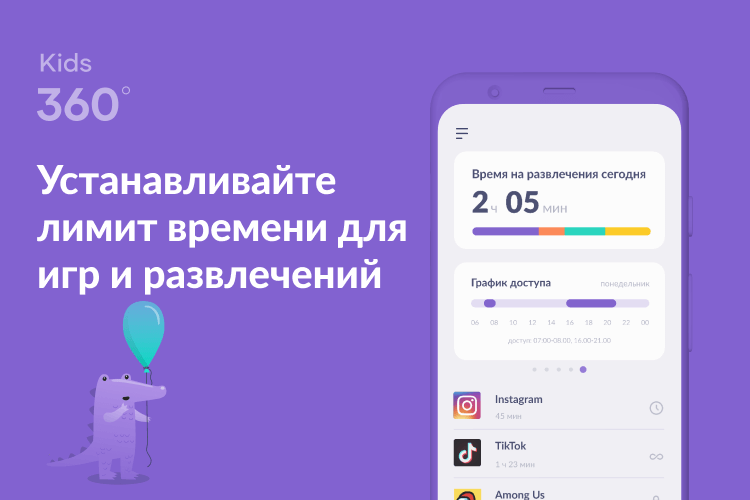
Prostock-studio/Shutterstock.com

Дети тоже становятся жертвами киберпреступников. Несовершеннолетних легче обманывать или пугать, проще выманить информацию и манипулировать. Превентивная защита работает лучше других способов.

Стоит поговорить с ребёнком и предупредить его о возможных опасностях в интернете. Задача — не запугать, а установить доверие и объяснить, на что стоит обращать внимание и как защитить себя от мошеннических действий, шантажа и вымогательства.

Чему важно научить ребёнка:

1. Не общаться с незнакомыми в сети.
2. Не рассказывать о личных и семейных средствах.
3. Если поступают угрозы, особенно такие фразы, как «родители узнают, если ты этого не сделаешь…», немедленно прекратить общение.
4. Любые контакты, которые вызывают неприятные эмоции — панику, страх, отвращение, — блокировать.
5. Не отправлять никому деньги, даже знакомым, возможно, их взломали.
6. Никому не рассказывать свои пароли и номера карт.



Prostock-studio/Shutterstock.com

Важно дать понять ребёнку, что он может поделиться с родителями, если происходит что-то неприятное, и его не будут наказывать, а постараются помочь. Оградить ребёнка от нежелательных сайтов, в том числе и тех, где могут действовать кибермошенники, также поможет родительский контроль. Это предупредит опасные действия злоумышленников в сети, направленные на детей.

Лучшее приложение родительского контроля — [Kids360](https://gdemoideti.ru/blog/exit.php?url=https://kids360.onelink.me/ykI8?pid=content_team&c=ru&af_channel=blog&af_adset=article&af_ad=kak-zashhitit-sebya-i-rebyonka-ot-kibermoshennikov;af_sub1=CTA). Кроме стандартной функции ограничения доступа к нежелательным приложениям, сервис отслеживает все действия маленького пользователя: составляет отчёты по статистике, из которых родитель узнаёт, какие программы ребёнок запускает чаще других, сколько времени в них проводит; а также помогает составлять расписание пользования гаджетом.

Однако помните, что перед тем, как установить родительский контроль, необходимо согласовать этот шаг с ребёнком. Объясните: это для его безопасности, а не для ограничения свободы.

Итоговый чек-лист



Prostock-studio/Shutterstock.com

Киберпреступность прошла долгий путь развития, и сегодня в арсенале мошенников масса способов по добыче банковских и личных данных граждан. Не говоря о способах использования этой информации для личной наживы.

Последствия для жертвы таких злоумышленников необратимы. Преступники не стесняются действовать через детей. Вы сможете уберечь себя и близких от кибермошенничества с помощью несложных методов кибербезопасности:

1. Ставьте защиту на телефон, компьютер и даже сим-карту. В случае утери или кражи устройства злоумышленники не смогут получить доступ к информации.
2. Не разглашайте информацию, связанную с паролями, счетами и банковскими картами. Мошенники любят представляться работниками банка и рассказывать, как с вашего счёта пытались увести деньги. Положите трубку и обратитесь по официальному номеру банковской организации, чтобы уточнить информацию.
3. Запоминайте пароли и не полагайтесь на автосохранение. Пароли должны быть надёжными и отличаться для каждого сайта. Закрывайте доступ к личным страницам от посторонних.
4. Не отвечайте на письма от сомнительных отправителей и не переходите по подозрительным ссылкам на опасные сайты. Установите антивирус: он не только защитит от вредоносного ПО, но и предупредит о подозрительном ресурсе.
5. Берегите детей от мошеннических действий. Предупредите об угрозах и расскажите, на что обращать внимание. Договоритесь о родительском контроле ради безопасности ребёнка.

Соблюдение большинства правил затрудняет взаимодействие с техникой. Но если вам есть что беречь, то лучше потерпеть небольшие неудобства, которые со временем станут привычными, а взамен обрести уверенное чувство безопасности. А главное — избежать неприятных проблем, последствий кибермошенничества.