Цифровая приватность.

Профили в социальных сетях, посты и комментарии представляют собой источник ценной информации для злоумышленников. Они могут использовать ее для реализации мошеннических схем, кражи денег, шантажа детей и родителей, кибербуллинга. Еще одна угроза, для которой недоброжелатели могут собирать данные о человеке, — доксинг. Это явление, при котором недоброжелатели делают публичной информацию о человеке, чтобы навредить ему и его репутации.

Чем больше данных о пользователе злоумышленник сможет найти, тем лучше может подготовиться. В основе многих мошеннических схем лежит социальная инженерия. Имена родственников, клички домашних животных, детали семейного быта и даже тех мест, в которых вы регулярно бываете, — все это дает возможность легче входить в доверие.Многие дети не менее охотно, чем взрослые делятся большим количеством информации о себе в интернете. Такая модель поведения получила название *овершеринг*.

Какую информацию взрослым и детям лучше не размещать в профиле в социальной сети:

номер школы, где сейчас учится ребенок;

домашний адрес;

подробную геолокацию, отметки о том, где часто бываете;

номер мобильного телефона;

фотографии и сканы документов, билетов на мероприятия, банковских карт;

фотографии дорогих покупок, обстановки в квартире;

откровенные фотографии — личные и близких людей.

Однако получить доступ к конфиденциальной информации злоумышленники могут, если украдут аккаунт человека в каком-либо сервисе, например социальной сети или мессенджере. Или если заразят его устройство вредоносной программой.

Чтобы защитить свою приватность, важно соблюдать определенные правила безопасности:

создавайте сложные и разные для каждой учетной записи пароли: от 12 знаков с заглавными и строчными буквами, цифрами, символами;

используйте защитные решения на всех устройствах;

установите двухфакторную аутентификацию в тех сервисах, которые это позволяют;

не переходите по сомнительным ссылкам, даже если их прислали знакомые;

не вводите данные от учетной записи на подозрительных сайтах;
добавляйте в друзья только тех пользователей, которых знаете лично.

Финансовая безопасность.

В интернете люди могут столкнуться с такими видами онлайн-мошенничества, как фишинг и скам.

Фишинг — это вид мошенничества, включающий в себя подделку страницы известной организации с целью украсть у пользователя его личные данные. Это может быть логин и пароль, данные банковской карты. В дальнейшем злоумышленники могут использовать полученные данные для кражи денег или чтобы получить доступ к другой конфиденциальной информации.

Скам — вид онлайн-мошенничества, при котором пользователю предлагают щедрое денежное вознаграждение или ценный приз. Чтобы его получить, просят оплатить комиссию, обычно небольшую. Комиссия достается злоумышленникам, а человек не получает ничего. Если же для перевода комиссии пользователь вводит данные карты, то рискует и их сохранностью.

Злоумышленники создают большое количество фишинговых ресурсов, которые подделываются под крупные, узнаваемые онлайн-магазины, платежные сервисы, социальные сети, мессенджеры. В случае с онлайн-магазинами мошенники могут заманивать пользователей закрытыми распродажами, уникальными предложениями и большими скидками. В случае с социальными сетями или платежными сервисами они могут пугать пользователей тем, что кто-то посторонний якобы пытается получить доступ к аккаунту, или просить подтвердить данные для входа. Как только человек вводит на фишинговой странице конфиденциальные данные, они уходят злоумышленникам.

Когда речь идет о скаме, злоумышленники обычно предлагают получить выплату, социальное пособие или принять участие в беспроигрышной лотерее. В любом случае пользователю обещают щедрый приз. Чтобы его получить, не нужно сложных действий: достаточно кликнуть пару раз на сайте или пройти небольшой опрос.

Чтобы не попяться на удочку мошенников, рекомендуем соблюдать основные правила кибербезопасности:

не переходите по сомнительным ссылкам из почты, сообщений в мессенджерах и СМС;

не сообщайте третьим лицам, даже если они представляются по телефону или в интернете сотрудниками банков или госучреждений, конфиденциальную информацию, в том числе одноразовый код из СМС и push-уведомлений;
используйте надежное защитное решение, которое предупредит, если человек попытается перейти на фишинговый или скам-ресурс;
если вас просят сделать что-то быстро, не дают времени подумать, пугают или, наоборот, делают крайне щедрые предложения, — стоит насторожиться;
ресурс, прежде чем вводить на нем свои данные, следует проверить: обратите внимание на название ресурса в адресной строке (соответствует ли оно официальному), работают ли кнопки на сайте, нет ли опечаток или несоответствий настоящему сайту.

Мобильные угрозы.

Мы храним большое количество данных на смартфонах, общаемся и обмениваемся информацией с помощью мобильных устройств. Не удивительно, что интерес к ним со стороны злоумышленников постоянно растет.
Пользователи смартфонов могут столкнуться с самыми разными киберугрозами: скамерскими приложениями, сталкерским ПО, программами-шпионами и другими троянцами, нежелательной рекламой, различными видами онлайн-мошенничества: фишингом, скамом. Актуальной угрозой остается телефонное мошенничество.
Распространяют вредоносные программы злоумышленники чаще всего на неофициальных площадках с приложениями. Однако это не единственные ресурсы, где человек может с ними столкнуться. Порой бывает так, что зловредные приложения проникают и в официальные магазины (как правило их оперативно удаляют). Злоумышленники присылают ссылки на такие приложения в социальных сетях, почте, мессенджерах.
Зачастую вредоносные программы никак себя не выдают. Есть ряд признаков, лишь косвенно намекающих на заражение, например крайне активно расходуется интернет-трафик, быстро разряжается батарея. Но однозначно ответить на вопрос, заражено ли устройство, можно только с помощью антивирусных решений.
Чтобы не столкнуться с вредоносным ПО, мы рекомендуем пользователям смартфонов:
скачивать приложения только из официальных магазинов;

перед запуском скачанных файлов проверять их при помощи антивирусной программы;
регулярно обновлять приложения и операционную систему — вместе с обновлениями разработчики выпускают исправления уязвимостей и ошибок;
обращать внимание на то, какие разрешения выдаете приложению, например приложению «Фонарик» явно не нужен доступ к контактам или геопозиции;
использовать надежное защитное решение (антивирус);
не переходить по подозрительным ссылкам, даже если их прислали знакомые.

Фишинговые ссылки.

Цель мошенников — получить доступ к сохраненным паролям или данным банковской карты жертвы. Незнакомец присылает ссылку на сайт для покупки товаров или услуг: через этот сайт злоумышленник получает нужную ему информацию.
Мошенничество с помощью поддельных сайтов называется **фишингом**.
Если вам еще не исполнилось 18 лет и вы попались на фишинг, обязательно сообщите взрослым – они вас поймут и помогут предпринять необходимые действия.
Как не стать жертвой мошенников: правила безопасного поведения
Проверяйте подлинность сайтов и вводите данные только на официальных страницах.
Прежде чем знакомиться в социальных сетях, внимательно изучите страницу пользователя.
Покупайте билеты и услуги на официальных сайтах. Не переходите по ссылкам от малознакомых людей.
Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные: пароли, номер карты и так далее.
Перед тем, как ввести свои данные, проверьте адрес сайта в адресной строке.
Сравните предлагаемую цену с другими сайтами: обычно цены на фишинговых сайтах подозрительно низкие.
Что делать, если вы стали жертвой мошенников
Воспользуйтесь функцией «Пожаловаться» или «Добавить в спам» в своем почтовом ящике.
Поговорите со взрослыми и обратитесь в полицию.
Чему нужно учиться:

внимательно изучать адресную строку сайта,
проверять информацию о новых онлайн-знакомых,
не торопиться совершать покупки на новых сайтах,
не доверять заманчивым предложениям,
не открывать сомнительные письма.

Ключевые правила:

помнить, что в сети много мошенников,
если есть сомнения, советоваться с кем-нибудь старше и авторитетнее,
не торопиться с принятием решений, касающихся перевода денег,
проверять источник информации.

Защита личной информации.

Если вам еще не исполнилось 18 лет и ваши личные данные попали в руки мошенников, обязательно сообщите взрослым – они вас поймут и помогут предпринять необходимые действия.

Правила безопасного поведения: как не стать жертвой мошенников

Выделите время и разберитесь в настройках своего профиля во всех соцсетях.

Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др. Делясь важной или личной информацией, используйте фильтр «Только для друзей».

Защищайте всю информацию, даже если думаете, что она не важна.

Устанавливайте разные сложные пароли для разных ресурсов.

Чему нужно учиться:

соблюдать спокойствие в любой ситуации,
устанавливать разные сложные пароли для разных ресурсов,
не публиковать в сети данные паспорта и других документов,
не сообщать никому пин-код и CVV (три цифры на обороте) своей банковской карты,
следить, чтобы полные данные банковской карты не попали в сеть,
не выкладывать фотографии билетов на самолёт или поезд, а также билетов на мероприятия со штрихкодом.

Ключевые правила:

помнить, что в сети много мошенников,
если есть сомнения, советоваться с кем-нибудь старше и авторитетнее,
не торопиться с принятием решений, касающихся перевода денег,
предупреждать своих друзей и подписчиков в случае, если вашим профилем завладели злоумышленники.

Кибербуллинг.

Кибербуллинг — травля в интернете. Цель мошенников – психологическое давление или причинение морального вреда жертве.

Как противостоять агрессии

Помните, что травля может случиться с каждым и вашей вины в этом нет.

Найдите того, кто вас поддержит.

Больше общайтесь с теми, кто рядом с вами. Не отвечайте обидчикам и не вступайте в споры.

Заблокируйте всех, кто пишет вам неприятное.

Пожалуйтесь на контент с угрозами и оскорблениями, используя инструменты соцсети. Если вам угрожают, сделайте скриншоты таких сообщений.

Если вы столкнулись с кибербуллингом

Сохраняйте спокойствие и не вините себя.

Помните, что есть люди, которые готовы вам помочь.

Поговорите с родными, близкими друзьями или с психологом на линии помощи подросткам «Твоя территория» 8 (800) 200-01-22. Если вам еще не исполнилось 18 лет, обязательно сообщите взрослым, которым вы доверяете – они вас поймут и помогут предпринять необходимые действия.

Постарайтесь сохранить всех подтверждения агрессивного общения: скриншоты переписки, фото, видео.

Пожалуйтесь на публикации службе поддержки, модераторам. Обратитесь за помощью в профильный благотворительный фонд — найти их можно на kiberbulling.net. Если сообщения с угрозами продолжаются, важно попросить родителей или старших родственников обратиться в полицию и предоставить скриншоты, которые подтверждают ваши опасения.

Чему нужно учиться:

соблюдать спокойствие в любой ситуации,

ни с кем не делиться интимными фотографиями, общаться вежливо в любой ситуации,

не обижать и не оскорблять других.

Ключевые правила:

помнить, что в сети есть агрессивно настроенные пользователи,

если есть сомнения, советоваться со старшими родственниками, друзьями или родителями,
не публиковать персональные данные — например, домашний адрес, телефон, паспортные данные,
не поддаваться агрессии и не вестись на провокации,
не делиться личной информацией, которая может быть использована против вас,
не участвовать в травле, даже если друзья предлагают вам это.

Защита профиля.

Цель мошенников — завладеть вашими логином и паролем и, соответственно, вашим профилем или аккаунтом, чтобы вымогать деньги у вас или ваших подписчиков. Для базовой защиты своего профиля используйте двухфакторную аутентификацию: тогда для того, чтобы зайти в ваш аккаунт, нужно будет ввести не только пароль, но и код, который будет приходить вам на привязанный номер телефона.

Если вам еще не исполнилось 18 лет и ваш аккаунт взломали, обязательно сообщите взрослым – они вас поймут и помогут предпринять необходимые действия.

Правила безопасного поведения: как не стать жертвой мошенников

Используйте разные пароли на различных сервисах.
Выбирайте сложные пароли, а чтобы их было легко придумывать и хранить, используйте менеджеры паролей.
Не используйте ваши имя, фамилию и дату рождения при создании пароля. Настройте дополнительное подтверждение входа — двухфакторную аутентификацию, чтобы аккаунт не перешел в руки недоброжелателей.
Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить доступ к профилю в случае взлома будет проще.

Чему нужно учиться:

соблюдать спокойствие в любой ситуации,
устанавливать разные и сложные пароли на разных ресурсах,
использовать дополнительное подтверждение входа (двухфакторную аутентификацию), не переходить по незнакомым и подозрительным ссылкам.

Ключевые правила:

помнить, что в сети много мошенников,

если есть сомнения, советоваться с кем-нибудь старше и авторитетнее,
не торопиться с принятием решений, касающихся перевода денег,
написать в службу поддержку соцсети или иного ресурса и сообщить, что вашим аккаунтом завладели злоумышленники,
предупреждать своих друзей и подписчиков о том, что вашим профилем завладели злоумышленники.

Социальная инженерия.

Цель мошенников — с помощью психологических манипуляций побудить человека перевести деньги на их счет или совершить другие выгодные им действия.

Последнее время мошенники делают ставку не на технические средства взлома, а на знание психологии. Это называется **социальной инженерией**. Задача мошенника — вызвать у жертвы сильные эмоции, чтобы ею было проще управлять.

Как не стать жертвой мошенников: правила безопасного поведения

Никогда не переводите деньги незнакомым людям.
Если вы получили сообщение от незнакомца, попросите его поподробнее рассказать о себе.
Проверьте, действительно ли такой человек существует.
Попросите прислать больше информации о том, что вам предлагают.
Найдите официальный сайт компании, от лица которой выступает незнакомец, и уточните информацию у службы поддержки.
Не торопитесь принимать решение.

Что делать, если вы стали жертвой мошенников

Если вам еще не исполнилось 18 лет, обязательно сообщите взрослым – они вас поймут и помогут предпринять необходимые действия.
Обратитесь с заявлением в отдел полиции по месту жительства.
Сообщите о профиле мошенника в службу поддержки социальной сети, где получили сообщение.
Сообщите об инциденте в компанию, от лица которой выступал злоумышленник.

Чему нужно учиться:

соблюдать спокойствие в любой ситуации,
проверять информацию,
уточнять условия,
требовать договор, чек или акт, если приобретаете товар или услугу в интернете.

Ключевые правила:

помнить, что в сети много мошенников,
советоваться с кем-нибудь старше и авторитетнее, если есть сомнения, не торопиться с принятием решений, касающихся перевода денег.

Обучение детей учиться

КАК НАУЧИТЬ ДЕТЕЙ УЧИТЬСЯ?

РФ попала в топ-15 стран, наиболее зависимых от интернета, — средний россиянин проводит в онлайне 7 часов 17 минут в день. 66% пользователей предпочитают приложения интернет-магазинов, 65% — развлекательные сервисы или видеоприложения (например, YouTube), 47% — играют в мобильные игры. У 11% пользователей смартфонов установлены приложения для знакомств.

Что делать:

Проще всего начать осваивать информационную грамотность с интернета, ведь это самая динамичная и активно развивающаяся информационная среда. Постарайтесь показать ребёнку, что интернет — это не только место для развлечения и общения, но и это удобный инструмент для увлекательного освоения нового!

* Если вам еще не исполнилось 18 лет – ОБЯЗАТЕЛЬНО сообщите родителям (взрослым) – они вас поймут и поддержат.

Начините с собственного примера: чаще открывайте интересные и познавательные видео;
устраивайте виртуальные экскурсии для всей семьи в лучшие музеи мира;
снимите вместе с ребёнком ролик для YouTube или stop-motion анимацию;
предложите вместе послушать лекцию на тему, интересную ребёнку;
следите за новейшими научными открытиями и обсуждайте их дома.

Общение с детьми о цифровых навыках.

Одна из главных задач родителей, которые растят детей в эпоху цифровых технологий, — повысить свою цифровую компетентность и со знанием дела направлять ребенка.

По данным исследования Фонда развития интернета, 75% подростков обучались использованию мировой Сети самостоятельно и хаотично, в результате у детей отсутствуют систематизированные знания и целостное понимание того, как все устроено и работает.

Мы — последнее «аналоговое» поколение, растящее «цифровых» детей. И наша задача — постараться сократить «цифровой разрыв», стремиться узнавать больше о современных технологиях самим и помогать осваивать их детям. Особенно те, которые позволяют использовать цифровую реальность для творчества и саморазвития, а не только для игр.* Если вам еще не исполнилось 18 лет – ОБЯЗАТЕЛЬНО сообщите родителям (взрослым) – они вас поймут и поддержат.

Чему нужно учиться:

Снять страх перед «цифровым слабоумием» детей

Учить детей использовать Интернет для развития

Соблюдать родительский контроль

Ключевые правила:

Вместо того чтобы ругать ребенка, что он снимает чушь для YouTube, помогайте ему создавать контент. Придумывайте сюжеты, темы и собирайте факты.

Обучайте его элементарным цифровым навыкам с детства. И тогда он будет не только смотреть чужие сайты/игры/сервисы, но и создавать свои.

Помните, что цифровые навыки — это не только развлечения и игры, но и профориентация и билет в будущее.

Финансовая грамотность.

Необходимо иметь достаточный уровень знаний и навыков в области финансов, который позволяет правильно оценивать ситуацию на рынке и принимать разумные решения.

Низкий уровень финансовой грамотности и недостаточное понимание в области личных финансов может привести не только к банкротству, но и к неграмотному планированию выхода на пенсию, уязвимости к финансовым мошенничествам, чрезмерным долгам и социальным проблемам, включая депрессию и прочие личные проблемы.* Если вам еще не исполнилось 18 лет – ОБЯЗАТЕЛЬНО сообщите родителям (взрослым) – они вас поймут и поддержат.

Чему нужно учиться:

Как управлять личными финансами

Как говориться с детьми о деньгах

Как распознать мошенников