Будь осторожен онлайн!

Молодежь и цифровая безопасность

www.fingramota.by

GLOBAL MONEY WEEK

FINANCE DENMARK

ГРОШЫ ЛЮБЯЦЬ РАЗУМНЫХ ЛЮДЗЕЙ

Child&Youth Finance International

Для учителей: как пользоваться этим буклетом.
Буклет о цифровой безопасности включает много разделов. Выберите темы Вы хотели бы обсудить с учениками и организуйте в классе открытый диалог по этим вопросам.

Международная неделя финансовой грамотности детей и молодежи (Global Money Week) - это глобальная кампания, инициированная Международной организацией финансового образования детей и молодежи (Child & Youth Finance International). Во время этой недели проходят мероприятия, вдохновляющие детей и молодежь к познанию новой информации о деньгах, сбережениях, источниках средств к существованию, трудоустройстве и предпринимательстве. **Global Money Week** проходит ежегодно в марте в более 130 странах.

Узнай больше на: **www.globalmoneyweek.org**

Международная организация финансового образования детей и молодежи (Child & Youth Finance International, CYFI) – это международная организация по системной трансформации финансовых систем по всему миру в целях расширения экономических и социальных возможностей детей и молодежи. CYFI сотрудничает с партнерами из 130 стран мира.

Узнай больше на: **www.childfinanceinternational.org**

Этот буклет ”Будь осторожен онлайн! Молодежь и цифровая безопасность“ – отредактированная международная версия оригинального датского буклета ”Unge og Digital Sikkerhed“, который был разработан для Global Money Week в Дании в 2017 году.

Автор оригинальной версии: Troels Juel, консультант по финансовым вопросам из Дании.

Оригинальная версия написана при сотрудничестве ряда организаций и институтов Дании (Министерства финансов Дании, Полиции Дании, Агентства Дании по диджитализации, компании The e-mark, Совета по СМИ и делам детей и молодежи Дании).

Фото: Страница 1: Aleksandar Goergiev/Getty Images.
Страница 3: Maskot/Getty Images.
Странца 10: Bloom Productions/Getty Images.

Русскоязычная версия адаптирована и переведена специалистами Национального банка Республики Беларусь.

2017

ВВЕДЕНИЕ

Почему цифровая безопасность важна. В настоящее время люди проводят в сети значительную часть жизни. Когда ты делишься фотографиями в Instagram или через VK, переводишь деньги друзьям через мобильные приложения или покупаешь онлайн новые кроссовки или джинсы – все это происходит в цифровой среде.

Мир быстро движется в сторону цифровизации (диджитализации), постоянно появляются и становятся доступны всем нам новые возможности.

Однако важно, чтобы ты знал больше об этих новых возможностях и осознавал вызовы, которые они могут нести с собой. Новые вызовы могут включать все что угодно – начиная с правильного распоряжения деньгами онлайн, заканчивая созданием безопасного (уникального) пароля.

Этот буклет был создан, чтобы помочь тебе безопасно ориентироваться в цифровом мире денег. Запомни три основных правила, касающихся безопасности онлайн:

1. Руководствуйся здравым смыслом.

Если ты видишь необычную ссылку или веб-сайт, которые кажутся тебе небезопасными, проигнорируй – лучше их не посещать!

2. Если предложение кажется слишком хорошим, чтобы быть правдой, это, скорее всего, действительно, обман.

3. Не используй один и тот же пароль для всех своих аккаунтов.

Если ты используешь один и тот же пароль для всех своих онлайн аккаунтов, ты рискуешь стать крайне уязвимым в одно мгновение. Получив доступ к одному твоему аккаунту, злоумышленник сможет получить доступ ко всем твоим аккаунтам.

Мы дадим тебе еще нескольких простых советов в этом буклете. Не пойми нас неправильно, пользуйся любыми приложениями и социальными сетями. Интернет отличная вещь для общения с друзьями, поиска и обмена информацией. Цифровизация делает нашу жизнь проще и рациональнее. Но, пользуясь всеми этими технологиями, надо быть бдительным и позаботиться о своей безопасности в сети.
Этот буклет поможет тебе получить полезные практические знания для твоей цифровой безопасности!

Приятного чтения!

Child & Youth Finance International

СОДЕРЖАНИЕ

ПАРОЛЬ

КАК ПРИДУМАТЬ СЛОЖНЫЙ ПАРОЛЬ

Сложный пароль – залог твоей онлайн безопасности. Нельзя использовать свою личную информацию, когда придумываешь пароль, особенно если эта информация видна всем в твоем профиле в соцсетях. Другими словами, не используй название твоего любимого фильма, футбольной команды, имя мамы, кличку кота и т.д. Разумеется, твоя фамилия и день рождения тоже не самые удачные варианты для основы пароля. Кроме того, старайся избегать общеупотребляемых и легко угадываемых паролей. Два из наиболее часто употребляемых паролей это ”123456“ и ”пароль“.

Используй разные пароли

Если у тебя есть несколько разных онлайн аккаунтов, для каждого из них нужен отдельный пароль. Многим людям кажется, что слишком сложно запомнить все эти разные пароли – поэтому они используют один и тот же пароль для всех аккаунтов. На самом деле, чтобы запомнить пароли нужно просто немного попрактиковаться.

Если же ты используешь только один пароль для всех своих аккаунтов, то хакерам или ворам намного проще взломать их и причинить тебе серьезный вред.

Научись придумывать сложные пароли

Если ты хочешь придумать сложный пароль, то сделай его длинным – это важно. Твой пароль всегда должен быть как минимум 8 знаков, даже если сайт не требует этого. Кроме длины сложный пароль должен состоять из заглавных и прописных букв, чисел и символов. При такой комбинации знаков посторонним будет сложнее разгадать твой пароль. Не очень хорошая идея – создавать пароль путем набора русских слов при включенной английской раскладке. Хакеры уже давно создали специальный словарь, позволяющий перебирать такие пароли.

Придумывай фразы

Есть одна фишка, чтобы создать надежный пароль – попробуй придумать кодовую фразу вместо одного слова. Кодовая фраза – это короткая поговорка, часть песни или детская считалка, которую ты можешь использовать, чтобы создать сложный пароль.

Например, ты можешь использовать строчку из песни или только первые буквы ее каждого слова, чтобы создать кодовую фразу. Потом запиши ее в таком порядке, чтобы тебе было легче запомнить (напевай ее, когда печатаешь). Также можно использовать специальные символы, заглавные буквы и числа в разных частях пароля, а не только в начале или в конце. Например, ”НеНб!ПчОх!1“ (Никогда его не брошу, потому что он хороший) будет очень надежным паролем, который одновременно легко запомнить.

Пароль должен быть таким, чтобы тебе было легко его запомнить, а другим сложно угадать.

Создай безопасный графический ключ

Создавать надежные графические ключи на девайсах также важно, как сложные пароли с разными цифрами, буквами и символами. К сожалению, многие люди не устанавливают хорошие графические ключи. Например, 44 % всех графических ключей начинаются в левом верхнем углу, а 10 % ключей представляют собой форму первой буквы фамилии человека.

Надежный графический ключ состоит из пересекающихся друг с другом линий. Также важно отключить опцию ”сделать видимым“, чтобы никто не смог увидеть пароль (ключ), когда ты его вводишь.

ФАКТ: самые популярные пароли:

1. 123456
2. password
3. welcome
4. 55555
5. abc123
6. 123456789
7. 12345678
8. sunshine
9. princess
10. qwerty

ПОЧЕМУ КИБЕРПРЕСТУПНИКИ ОБМАНЫВАЮТ ЛЮДЕЙ?

Пытаясь получить доступ к чужой информации, киберпреступники становятся все более и более изобретательными, организованными, мыслят стратегически. Их методы изощренны, и иногда очень сложно сразу обнаружить их махинации. Кроме того, они постоянно придумывают новые способы обманывать людей. Атаки киберпреступников проводятся с целью заработка или шпионажа, а также с целью демонстрации силы атакующих.

Важно знать, что, к сожалению, онлайн мошенничество становится частью нашей повседневной жизни. Пароль – залог безопасности, именно он защищает твой компьютер от различных угроз извне, не дает злоумышленникам узнать конфиденциальную информацию и что-либо сделать с ней. Многие молодые люди не меняют пароли. Киберпреступники пользуются этим, как и тем, что люди часто ставят один и тот же пароль на свои разные аккаунты. Это значит, что преступнику нужно взломать только один пароль, чтобы получить доступ сразу к нескольким аккаунтам.

ФАКТ:
Не используй в качестве пароля свой день рождения или имена членов семьи и клички домашних питомцев. Посторонние люди могут слишком легко их отгадать.

ОБСУЖДЕНИЕ В КЛАССЕ:

Как сделать так, чтобы другим людям было сложно угадать твой пароль?

У тебя есть подозрения, что кто-то узнал твой пароль?
Если да, то смени его немедленно!

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НА ТВОЕМ МОБИЛЬНОМ ТЕЛЕФОНЕ, ПЛАНШЕТЕ И КОМПЬЮТЕРЕ

Что такое девайс?

Девайс – это общеупотребительный термин для компьютеров, смартфонов, планшетов и других ”умных“ электронных устройств. Слово ”девайс“ пришло к нам с английского языка, в переводе означает ”устройство, прибор“. Теперь оно активно используется и в нашем лексиконе в контексте ”какое-либо техническое устройство“.

Кто такие хакеры?

Хакеры – это взломщики, которые целенаправленно используют слабые места в системах безопасности различных девайсов, а также личных, профессиональных, коммерческих аккаунтов, чтобы получить доступ к информации, данным и фотографиям. А раньше так называли программистов, которые исправляли ошибки в программах, основываясь на собственных не совсем стандартных способах.

Что такое вредоносная программа?

Вредоносная программа – это общий термин для программ, которые наносят вред девайсам.

Ты пользуешься мобильным телефоном, планшетом и компьютером регулярно. Кроме того, твои возможности по их использованию постоянно растут. Например, теперь ты можешь не только общаться онлайн со своими друзьями и семьей, но и легко связаться со своим школьным учителем, доктором или банком через свой девайс.

Ты можешь делать покупки прямо через приложения на планшете и платить в супермаркете с помощью своего мобильного телефона. Есть несколько способов усложнить хакерам доступ к твоей личной информации или счетам. В этой части буклета описано, как защитить свои девайсы от вредоносных программ, вирусов и взлома.

ПОЛЕЗНЫЕ СОВЕТЫ И ФИШКИ, КАК ЗАЩИТИТЬ СВОИ ДЕВАЙСЫ ОТ ХАКЕРОВ И ВИРУСОВ:

Обновляй программное обеспечение

Большинство девайсов автоматически не обновляют приложения или программное обеспечение системы безопасности. Поэтому лучше самому следить за этим. К счастью, обновить приложения и программное обеспечение системы безопасности, чтобы поставить себе на девайсах самую последнюю защиту, обычно не занимает много времени. Обязательно обновляй програмное обеспечение на своих девайсах, если столкнешься с багами или вирусами.

Если на твоих девайсах не обновлено програмное обеспечение, они будут более уязвимы для хакеров, вредоносных программ и вирусных атак. Это значит, что посторонние лица могут украсть информацию с твоего девайса (например, пароли или данные платежной карты) или даже полностью контролировать твой девайс.

Используй антивирусы

Антивирусные программы защищают твои девайсы от вредоносных файлов. Есть бесплатные программы, которые ты можешь скачать и установить. Но если ты хочешь еще больше усилить защиту своих девайсов, ты можешь купить мощную эффективную антивирусную программу. Оплата антивирусных программ может быть разумной тратой денег, потому что платные антивирусы обычно имеют определенные опции, которые не доступны в бесплатных вариантах.

Будь осторожен при подключении к бесплатному Wi-Fi

Скорее всего, твои девайсы автоматически подключаются к wi-fi дома или в местах, где ты часто бываешь. Естественно, так намного легче, быстрее и удобнее. Также это удобный способ сохранять просмотренные данные. Когда ты находишься за городом или где-нибудь еще, бесплатный wi-fi кажется очень привлекательным. Однако важно использовать только те сети wi-fi, владельцу которых ты доверяешь. Если ты используешь бесплатную сеть wi-fi, владельца которой ты не знаешь, ты рискуешь тем, что посторонние люди смогут следить за твоими действиями в сети и перехватывать твою личную информацию.

Многие кафе и рестораны предлагают бесплатный доступ к открытым (незащищенным) сетям для своих клиентов. Если злоумышленники подключатся к этой открытой сети, они легко смогут получить доступ к информации, которая отправляется на твой девайс и с него и воспользоваться ей. Поэтому следует быть очень осторожным по отношению к wi-fi сети и незащищенному каналу, к которым ты подключаешься.

Знаешь ли ты, что загружаешь?

Возможно, ты часто загружаешь новые приложения на мобильный телефон, планшет и компьютер. Когда ты используешь авторизованные сервисы, такие как Appstore и Google Play, для загрузки новых приложений, ты можешь быть вполне уверен, что они не содержат вирусы или вредоносное программное обеспечение. Но важно знать, что не все приложения и программы через авторизированные сервисы тщательно проверяются на наличие вирусов и вредоносного програмного обеспечения.

Не рекомендуется загружать приложения и программы прямо по ссылкам в электронной почте и сообщениях, так как они могут содержать вирусы и вредоносное программное обеспечение. Кроме того, если что-то предлагается бесплатно, но ты знаешь, что обычно это стоит денег, то будь осторожен. Возможно тебе предлагают программу, которая содержит вирусы или вредоносное программное обеспечение. Бесплатный сыр бывает только в мышеловке!

Разрешения для приложений

Когда загружаешь приложения, у тебя могут запрашивать согласие на доступ к информации из твоего девайса. Некоторые приложения могут спросить разрешение на действия, которые не нужны для работы приложения. Иногда это может быть доступ к твоей камере или микрофону на неограниченное время. Полезно следить за установкой приложения на девайсе, чтобы видеть, на что ты даешь разрешение.

ОБСУДИТЕ В КЛАССЕ:

Почему необходимо обновлять девайсы?

Как часто их надо обновлять?

Подумай, какие беспроводные сети стоит и не стоит использовать?

Ты знаешь кого-нибудь, чей компьютер взломали? Как это произошло?

Как ты изменишь свое поведение при использовании девайсов?

Какой совет ты можешь дать другим?

Как ты можешь безопасно использовать свои девайсы?

ЭЛЕКТРОННЫЕ ДЕНЬГИ

ПОЗАБОТЬСЯ О СВОИХ ДЕНЬГАХ ОНЛАЙН

Сейчас деньги используются не только в физической форме, все чаще деньги используются в электронном виде. Многие люди сейчас используют интернет-банкинг и мобильный банкинг. С помощью интернет- и мобильного банкинга можно легко и удобно пересылать деньги другим людям, оплачивать счета и/или переводить деньги со счета на счет. Мобильные банкинги отличаются друг от друга, но обычно все они требуют определенный идентификационный номер, чтобы совершать операции с деньгами.

Важно убедиться, что посторонние люди не могут использовать твое веб- или мобильное приложение. Для этого сделай так, чтобы никто не знал твои пароли, секретные вопросы и ответы на них или другие коды.

ОПЛАТА ЧЕРЕЗ МОБИЛЬНЫЙ ТЕЛЕФОН

Когда ты отправляешь деньги через электронные устройства, каждый раз убедись, что они были направлены нужному получателю. Кроме того, обязательно проверь, правильно ли ты ввел сумму. Обидно и накладно нечаянно отправить 250 рублей, когда ты хотел перевести всего лишь 25 рублей. Всегда помни, что необходимо дважды проверять правильность информации при онлайн платежах. Мобильные способы оплаты являются личными и должны быть использованы только тобой. Поэтому, даже если ты полностью доверяешь кому-то, нельзя давать ему доступ к твоему телефону, в особенности, когда ты не видишь, что он делает.

Будь осторожен с пин-кодом

Нужно правильно выбирать пин-код для своих платежных приложений. Важно убедиться, что никто не знает твой пин-код (например, нельзя записывать его или хранить в записях своего телефона).

Также неразумно фотографировать свой пин-код и хранить его в фотогалерее в телефоне. Для хакеров будет подарком натолкнуться на твой пин-код, если они получат доступ к твоему телефону.

Если кто-нибудь взломает твой мобильный, он мгновенно получит доступ ко всем кодам, которые ты сфотографировал, если ты их сохранил в телефоне.

ПЛАТЕЖНЫЕ КАРТЫ

Дебетовая карта может быть использована для покупок в таких местах, как магазины, онлайн магазины или для снятия денег из банкомата.

Платежная карта является личной и имеет 4-значный пин-код, который вводится при ее использовании. Важно, чтобы другие люди не знали твой пин-код. Убедись, например, что другие люди не видят его, стоя у тебя за спиной, когда ты его вводишь в магазине. Разумно прикрывать рукой клавиатуру, когда ты вводишь пин-код, особенно, когда за тобой очередь. Как и при онлайн покупках, рекомендуется проверять, что сумма оплаты действительно соответствует стоимости покупки. Большинство продавцов и кассиров, конечно, порядочные люди и им можно доверять. Но, тем не менее, доверяй, но проверяй! Если тебе попадется непорядочный человек, он может добавить дополнительную сумму тебе в чек. Поэтому всегда нужно проверять сумму, которую ты оплачиваешь и сохранять чек после покупки.

Если ты потеряешь свою дебетовую карту, либо у тебя появится подозрение, что твой счет был скопроментирован, немедленно обратись в свой обслуживающий банк.

Какие виды оплаты ты знаешь?

Есть разные виды банковских платежных карточек. Самые распространенные – дебетовая и кредитная.

При использовании **дебетовой карты** деньги списываются с твоего счета в банке. С дебетовой карты можно снять только те деньги, которые ты сам (или кто-то еще) на нее положил. Одной из самых популярных разновидностей дебетовых карточек являются зарплатные карточки.

Некоторые банки предлагают дебетовые карты с возможностью овердрафта. Слово «овердрафт» переводится с английского языка (overdraft) как «перерасход», либо «сверх плана». Эта фишка позволяет тебе тратить больше, чем имеется у тебя на счете. Услуга эта предоставляется банком не бесплатно – на сумму фактически израсходованных средств банк начисляет проценты.

Кредитная карта похожа на дебетовую тем, что с ее помощью также можно совершать покупки в магазинах и онлайн без использования наличных средств. Однако она не списывает деньги непосредственно с твоего счета. Вместо этого используются деньги банка, который предоставил тебе кредитную карту, и ты должен будешь вернуть ему эти деньги через определенный промежуток времени.

Также надо обязательно помнить, что за пользование кредитными деньгами тебе необходимо будет заплатить банку процент.

Ты потерял свою платежную карту или подозреваешь, что она была скомпрометирована?
Если да, то срочно звони в свой банк.

ОНЛАЙН ШОПИНГ

Все больше и больше людей во всем мире предпочитают покупки в интернете обычным магазинам. Потому что делать это из дома удобнее, легче найти последние новинки и выгодные предложения. К сожалению, мир онлайн шопинга – это тоже место, где жулики могут обмануть покупателей, особенно тех, кто не руководствуется здравым смыслом при покупке товаров. Поэтому мы написали восемь советов, которые помогут тебе избежать негативного опыта при онлайн шопинге.

Проверь, где территориально расположен интернет-магазин

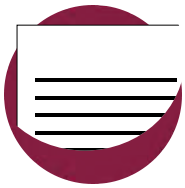
Ты посещаешь интернет-магазины, которые находятся за пределами Беларуси? Если да, то тебе стоит знать, что возможно надо будет платить таможенные пошлины. При оплате таможенных пошлин твоя покупка станет несколько дороже, чем ты ожидал. Следовательно, то, что изначально было выгодным предложением, может оказаться в итоге вовсе невыгодным. Помни об этом, когда совершаешь покупки в интернете.

Посмотри на замочек в адресной строке

Есть ли маленький замочек возле веб-адреса интернет-магазина? Этот замочек означает, что информация, которую ты вводишь о себе и твоих способах оплаты, передается через безопасный канал связи или через защищенное соединение. Не делай покупок в интернет-магазинах, которые не имеют этого замочка рядом с веб-адресом.

Почитай отзывы других покупателей об интернет-магазине и продукте

Если ты нашел нужный продукт по хорошей цене, будет полезно потратить немного времени, почитав, что говорят предыдущие покупатели об этом товаре и интернет-магазине. Поэтому желательно посмотреть отзывы о товаре на сайте самого магазина и на других сайтах о нем. Не забывай, что онлайн- рейтингом можно манипулировать, поэтому необходимо руководствоваться здравым смыслом, изучая отзывы других людей. Более того, никогда не делай свой выбор только на отзывах пользователей. Рассматривай отзывы как дополнительную информацию для принятия решения. Если тебе кажется что-то подозрительным в интернет-магазине или товаре, то спроси совета у взрослого, которому ты доверяешь, либо поищи на другом сайте.



Всегда читай то, с чем соглашаешься

Может быть, это не очень интересно, но ты должен всегда читать условия, на которых ты совершаешь онлайн-покупки. На каждом сайте они разные. Особенно, когда речь идет о подробностях оплаты, подачи жалобы или особых условиях, касающихся доставки. Также следует изучить условия возврата и обмена товара перед тем как сделать покупку.

Знай свои права

В Беларуси у тебя есть 14 дней на то, чтобы вернуть товар, приобретенный в сети. Это значит, что ты можешь поменять или вернуть деньги за туфли, которые ты купил, если они оказались слишком большие или по любой другой причине при условии, что они будут новые, и если ты сделаешь это в установленный срок.

Но помни, что обычно нужно оплачивать стоимость обратной пересылки продавцу, если ты передумал или ошибся с выбором.

Имей отдельную карточку

Для оплаты товаров в интернете лучше использовать отдельную карточку, к отдельному счету и с ограниченной суммой денежных средств на нем, предназначенную только для данной покупки.

Не сохраняй данные карточки

Не стоит позволять браузерам сохранять данные карточки «для упрощения совершения покупок в будущем».

Сохраняй квитанцию

Если товар, который ты купил, сломается, скажем, через пять дней, ты можешь заменить его или получить возмещение денег только в том случае, если ты сохранил квитанцию об оплате и/или бланк подтверждения заказа из онлайн магазина. Сохрани любые электронные документы, переписку по электронной почте и квитанцию об оплате в течение как минимум двух лет, в особенности, если ты приобрел дорогостоящую вещь.

ОБСУДИТЕ В КЛАССЕ:

Ты когда-нибудь делал покупки в интернет-магазине? Расскажи о своем опыте.

ОБСУДИТЕ В КЛАССЕ:

Слышал ли ты, что кого-то обманули в интернет-магазине? Как это произошло?

Научись определять фейковый магазин!

Большинство онлайн-покупок осуществляется без проблем. Однако, всегда есть исключения. Мошенники и тут могут попытаться обмануть тебя. К счастью, большинство схем мошенников легко определить, особенно если ты знаешь, что искать. Существует несколько признаков, свидетельствующих, что интернет-магазин фейковый. Если ты заметишь их, то держись от него подальше:

Цены в магазине слишком привлекательные

Что должно смутить опытного покупателя, так это не реальные скидки! Многие мошенники предлагают очень выгодные цены на якобы брендовые товары. Мошенники могут запросить цену в 10 евро за пару кроссовок, которые обычно стоят 100 евро, чтобы получить быстрые и легкие деньги.

Стилистические или грамматические ошибки

Многие фейковые магазины переводят текст сайта с одного языка на другой с помощь программ машинного перевода, поэтому если ты видишь, что в описании товара много грамматических ошибок или опечаток, лучше покинуть этот сайт.

Подозрительное имя сайта

Сами доменные имена мошеннических сайтов, как правило, длинные и сложные, могут читаться справа-налево или в адресной строке отображается одинаковый адрес для всех страниц сайта. Проверяй, чтобы адрес сайта соответствовал названию интернет-магазина.

Контакты

Просмотрите контакты на предмет наличия городских телефонов. Как правило, настоящие интернет-магазины имеют несколько телефонов, в том числе городских. Желательно наличие фактического адреса (склада или офиса).

Никогда не вводи логин, пароль, адрес электронной почты, номер банковской карты и другую личную информацию пока окончательно не убедишся в подлинности интернет ресурса.

СОЦИАЛЬНЫЕ СЕТИ

ПРАВИЛЬНОЕ ПОВЕДЕНИЕ В СОЦИАЛЬНЫХ СЕТЯХ

ОБСУДИТЕ В КЛАССЕ:

Обсудите в классе, какими социальными сетями пользуются ученики, почему они ими пользуются и как вести себя правильно в социальных сетях, по их мнению. Что они слышали о положительном и отрицательном опыте пользования социальными сетями.

Большинство людей пользуются социальными сетями и имеют аккаунты на двух и более платформах. Даже если у тебя нет аккаунтов ни в каких социальных сетях, ты, наверное, много о них слышал. Когда ты находишься онлайн, всегда важно думать, что ты пишешь, потому что это смогут увидеть посторонние люди или потом поделиться твоей записью без твоего ведома. Нужно придерживаться правила: не писать онлайн ничего такого, чего бы не сказал вслух на публике. Даже если ты шутишь, другие могут неправильно интерпретировать твой юмор. Кроме того, что ты говоришь, думай, какую информацию ты выкладываешь онлайн, не показывай личную информацию, не делись и не делай репост фото или видео без разрешения людей, которые на них изображены.

БЕСПЛАТНЫ ЛИ СОЦИАЛЬНЫЕ СЕТИ

Создание аккаунта бесплатно в большинстве социальных сетей.

Однако эти сети принадлежат частным компаниям, которые стремятся получить максимальную прибыль. Один из способов заработать деньги, это собрать информацию о тебе – например, о твоих привычках посещения сайтов, чтобы показывать тебе наиболее целевые объявления. Информация, которую ты предоставляешь, когда создаешь профиль на их сайте и вся информация, которую ты предоставляешь, когда общаешься в социальных сетях, создает твой цифровой след (например, посты, которые ты лайкаешь, на которые ты переходишь, которые ты комментируешь или репостишь) и постоянно отслеживается, сохраняется и используется. Платформы социальных сетей используют твои данные, чтобы составить твой портрет, который позволит им предлагать тебе определенный контент и рекламу.

ВОЗЬМИ ПОД КОНТРОЛЬ СВОЮ ЦИФРОВУЮ ЖИЗНЬ

Когда ты создаешь аккаунт в социальных сетях, настройки твоего профиля по умолчанию установлены так, чтобы тебя могли видеть все. Важно, чтобы ты осознавал это и следил за тем, какой информацией ты делишься в социальных сетях и вообще в интернете. Чтобы незнакомые люди не могли видеть, что ты выкладываешь, измени настройки приватности в твоем профиле, чтобы только ”друзья“ или ”подписчики“ могли видеть твой профиль и контент, которым ты делишься. Ты также должен подумать, нужно ли тебе делиться такой информацией, как школа, в которой ты учился, дата рождения, телефонный номер. Если в этом нет необходимости, разумнее не показывать ее.

Не очень разумно везде сообщать эту информацию. Также нужно дважды подумать перед тем, как выложить что-нибудь в интернет. Даже если ты сразу удалишь то, что ты написал или чем поделился, никогда нельзя быть полностью уверенным в том, что информация полностью уничтожена, и кто-то другой не сохранил ее, пока она была онлайн.

ПОЛЕЗНЫЕ СОВЕТЫ

Всегда проверяй, что изменил настройки социальных сетей так, чтобы только друзья или подписчики могли видеть твой пост. Также помни, что ты можешь заблокировать определенных людей или группу людей, которые не смогут видеть твой профиль.

В сети говори однозначно и используй точные выражения, чтобы не возникло недопонимания, что часто случается, когда люди не разговаривают тет-а-тет. Дважды думай, когда ставишь лайки, комментируешь или делаешь репост, так как слухи или ложь могут очень быстро распространиться и испортить твою репутацию.

Не делись даже с близкими людьми, друзьями своими фотографиями и видео, которые ты не хотел бы, чтобы видели окружающие. Их легко сохранить или поделиться ими без твоего ведома. Даже если у тебя сейчас надежные и хорошие отношение с этим человеком, не обязательно вы сохраните их и в течение всей жизни.

Никогда не делись и не пересылай личные фото или видео других людей без их явно выраженного согласия, даже если ты думаешь, что эти фото милые или забавные. Человек на фото или видео может стесняться их, или просто не хочет, чтобы они оказались в интернете. Всегда спрашивай разрешения перед фотографированием и распространением. Также уважай мнение других людей, если они говорят ”нет“.

Всегда легко увлечься и выложить забавное, волнующее или сексуальное фото или комментарий. Однако, как всегда, подумай дважды перед тем, как делиться чем-либо. Если ты пожалел о комментарии или фото, удали его немедленно. Если ты поделился с другими, попроси их тоже удалить его. Ты можешь всегда попросить друга, членов семьи или учителя тебе помочь. Не забудь извиниться, если ты сделал что-то неправильное или задел чувства других.

www.globalmoneyweek.org

www.childfinanceinternational.org

www.fingramota.by

GLOBAL MONEY WEEK

FINANCE DENMARK

ГРОШЫ ЛЮБЯЦЬ РАЗУМНЫХ ЛЮДЗЕЙ

Child & Youth Finance International