БУДЬ ОСТОРОЖЕН В МИРЕ IT!

НАУЧИСЬ ЗАЩИЩАТЬ СЕБЯ И СВОИ ДАННЫЕ.

RIIGI INFOSÜSTEEMI AMET

Наиболее важные термины

Login – вход

Logout – выход

MFA – многофакторный вход

2FA, two-factor authentication – двухэтапная аутентификация (в том числе двухфакторная аутентификация)

Password – пароль

IoT (Internet of Things) – Интернет вещей

Update – обновление, обновить

Backup – создание резервной копии

Accept – акцептировать, принять

Cancel – отмена, отменить

Settings – настройки

Phishing – фишинг, выманивание данных

Malware – вредоносное программное обеспечение

Ransomware – Программы-вымогатели

Firewall – брандмауэр

Encryption – шифрование

VPN (Virtual Private Network) – VPN, виртуальная частная сеть

Spyware – шпионская программа

Social engineering – социальные манипуляции

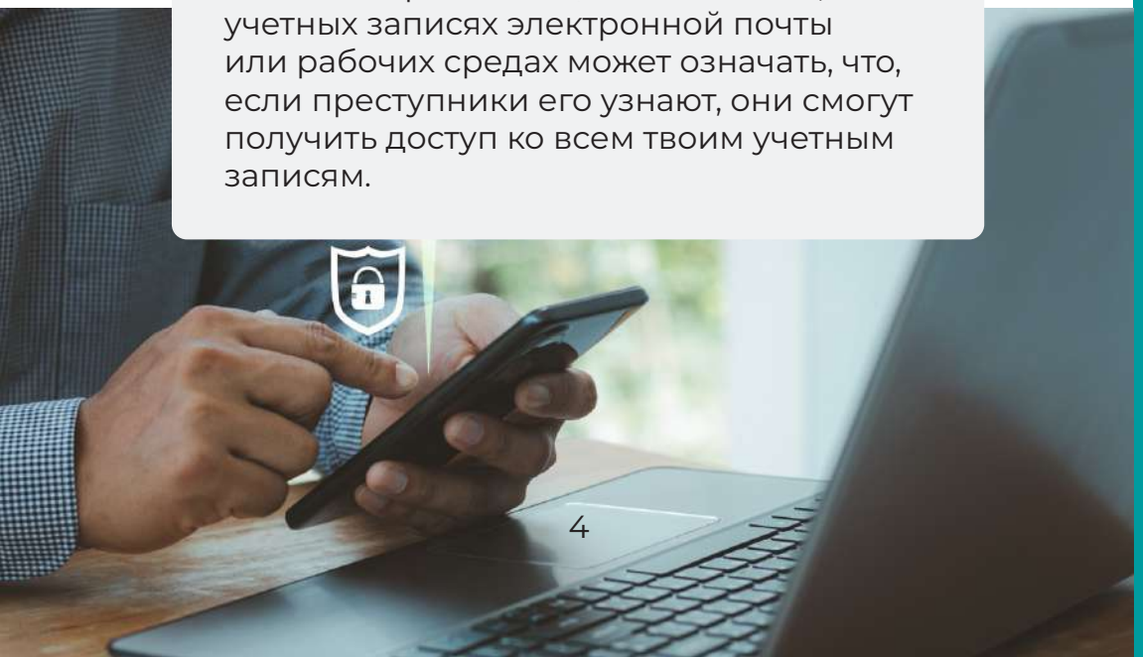
ПО – программное обеспечение

Содержание

1. Используй надежные, уникальные пароли и двухэтапную аутентификацию

Пароли используются для защиты твоих данных.

Использование одного и того же слабого пароля в социальных сетях, учетных записях электронной почты или рабочих средах может означать, что, если преступники его узнают, они смогут получить доступ ко всем твоим учетным записям.



Запомни!

1. Используй разные пароли для своей электронной почты, социальных сетей и рабочих учетных записей.
2. **Надежный пароль имеет длину не менее 12 символов и содержит буквы верхнего и нижнего регистра, цифры и специальные символы.**
3. Так же, везде, где это возможно, используй двухэтапный вход в систему, поскольку он обеспечивает дополнительный уровень безопасности в дополнение к надежному паролю.
4. Как его активировать? На большинстве платформ, таких как Facebook или Gmail, необходимо перейти в правый верхний угол, где можно просмотреть настройки своей учетной записи. Выбери там настройки безопасности и найди двухэтапную аутентификацию.
5. Выбери подходящий способ, например SMS, затем введи номер телефона и подтверди свой номер согласно инструкции.
6. Кроме того, можно использовать отдельное приложение для кодов безопасности.

2. Обновляй программное обеспечение на разных устройствах

Чтобы защитить устройства и данные, необходимо постоянно обновлять программное обеспечение.

Компьютер или смартфон с устаревшим программным обеспечением — привлекательная цель для киберпреступников.

Используя дыры в безопасности, можно заразить устройство вредоносным ПО и следить за действиями пользователя, сохранять пароли или получать доступ к другим данным.

Запомни!

1. В большинстве случаев обновление производится настолько просто, что не потребует больше усилий, чем несколько щелчков мыши. Если смарт-устройство или компьютер предлагает обновление, сделай небольшой перерыв и дай компьютеру сделать это.
2. **Всегда обновляйте все приложения на всех устройствах.**
3. Время от времени критически оценивай приложения, установленные на устройстве, и удаляй те, которыми больше не пользуешься.

3. Будь осторожен с неизвестными ссылками

Научись распознавать ссылки и файлы, которые могут оказаться опасными.

Прежде всего, нужно знать, что подозрительная ссылка может прийти из знакомого места. Например, от организации через SMS, от друга по электронной почте и от члена семьи через Messenger, WhatsApp или любое другой распространенный мессенджер.

В большинстве случаев текст рядом со ссылкой предлагает перейти по ссылке и ввести данные банковской карты, пароли или установить вредоносное ПО на свой компьютер.

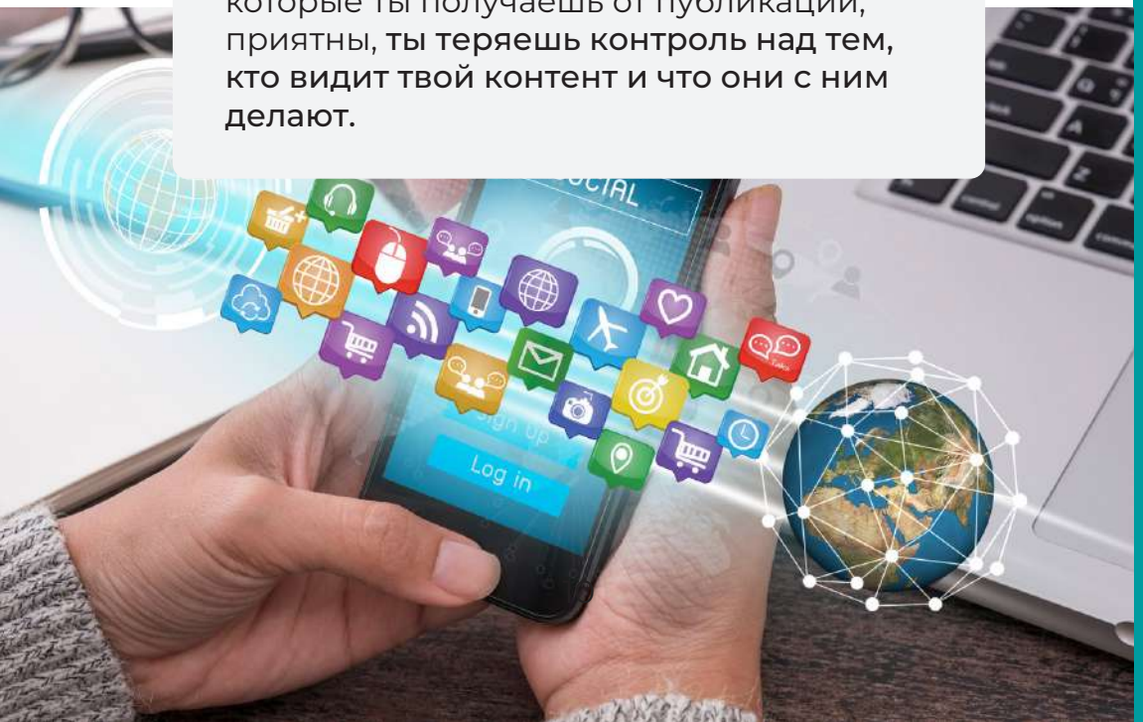
Запомни!

1. **Будь осторожен и не открывай на своем компьютере файлы прикрепленные к неизвестному письму.**
2. Если где-то в письме или СМС есть ссылка для входа, не кликай, а сам найди нужную веб-страницу в поисковике. В случае сомнений можно позвонить в службу поддержки клиентов.
3. Если ссылка пришла от кого-то из знакомых, но он обычно не присылает подобные материалы, спроси его по другому каналу, о чем речь. Например, позвони, потому что его аккаунт мог быть взломан.
4. Если все-таки нажимаешь, то не вводи конфиденциальную информацию и не разрешай установку или загрузку чего-либо.

4. Проверь настройки безопасности социальных сетей

Помните, что все в социальных сетях по умолчанию является общедоступным.

Даже если непосредственные эмоции, которые ты получаешь от публикации, приятны, **ты теряешь контроль над тем, кто видит твой контент и что они с ним делают.**



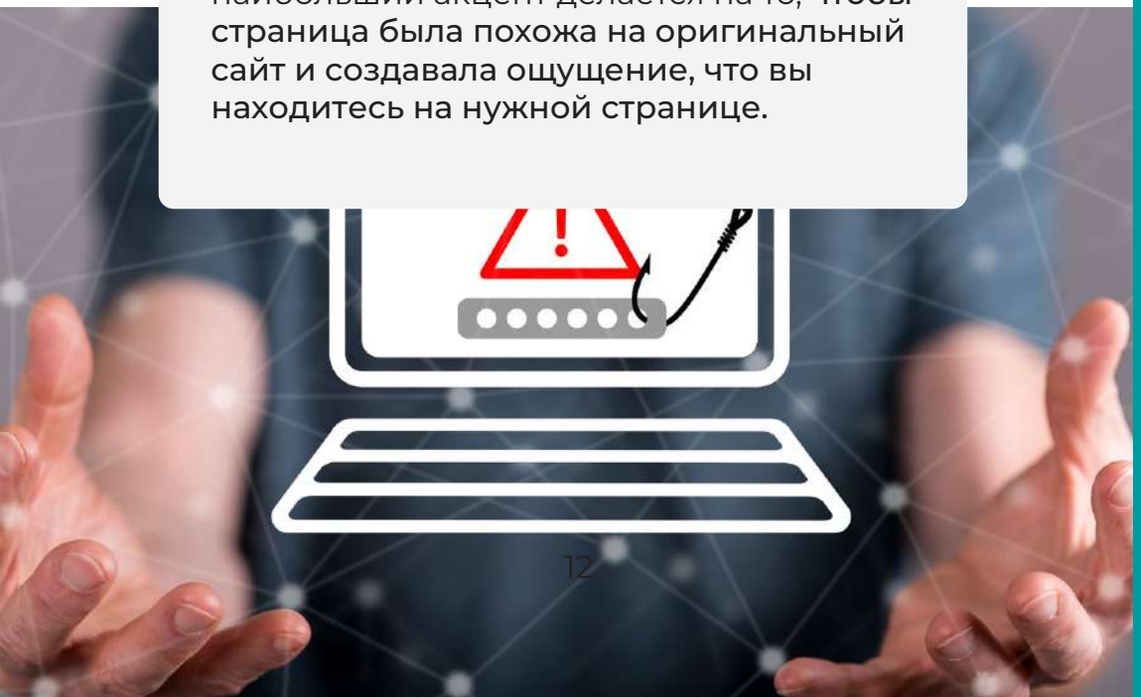
Запомни!

1. Используй двухэтапную аутентификацию и уникальный пароль в социальных сетях.
2. **Ограничь круг людей, которые могут видеть твои публикации и делиться ими.**
3. Добавляй в друзья только тех, кого ты действительно знаешь.
4. Не открывай ссылки неизвестного происхождения.

5. Научись распознавать фишинговые страницы

Цель фишинговых страниц — украсть данные вашей учетной записи или кредитной карты.

При создании фишинговых страниц наибольший акцент делается на то, **чтобы страница была похожа на оригинальный сайт и создавала ощущение, что вы находитесь на нужной странице.**



Запомни!

1. Прежде чем спешить с вводом своей информации, убедись, что адрес сайта, на котором ты находишься, именно такой, каким он должен быть (google.com вместо g00gle.com).

2. Если, к сожалению, ввёл свою пользовательскую информацию на фишинговой странице то:

   - **сразу же измени пароль своей учетной записи**
   - выйди из всех устройств, на которых зарегистрирована учетная запись
   - убедись, что у тебя активирована двухэтапная аутентификация.

6. Делай резервное копирование своих данных

Может случиться так, что компьютер сломается, пропадет или заразится вирусом, что делает твои важные файлы, такие как семейные фотографии и видео, непригодными для использования.

Единственный простой способ защитить свои данные — создать их **резервную копию.**

Данные можно сохранить. Это означает, что ты можешь довольно легко создавать резервные копии своих документов или изображений.

Запомни!

Существует два распространенных способа резервного копирования данных.

1. **Один из вариантов — скопировать всё важное на внешний носитель. Например, на карту памяти или жесткий диск.**
2. Другой вариант — выполнить резервное копирование в облачный сервис, который автоматически создает резервные копии твоих файлов.
3. Облачные сервисы часто предлагают бесплатное пространство для хранения (например, Google Drive, Microsoft OneDrive и т. д.).
4. Обязательно регулярно создавай резервные копии и убедись, что всё работает.

7. Изменяй заводские пароли устройства

Сегодня очень распространены пылесосы, часы, газонокосилки, принтеры, телевизоры и ряд других смарт-устройств, подключенных к Интернету.

Все эти устройства подключаются к Интернету с помощью роутера.

Если домашний роутер использует заводской пароль, какой-нибудь злоумышленник может завладеть им и в любой момент распечатать тысячи фотографий кошек или заставить твой телевизор включиться, нарушив твоё душевное спокойствие.

В худшем случае твой роутер, и подключенные к нему устройства, могут стать оружием для атаки на школу или местную больницу.

Запомни!

1. **Важно изменить заводской пароль роутера и проверить другие настройки безопасности.**
2. Также важно с самого начала проверять настройки безопасности и заводские пароли при работе с любым новым устройством.
3. Как это сделать? Эту информацию можно найти в инструкции к устройству. Если руководства нет в комплекте, выполни поиск в Интернете по названию и модели устройства.

8. Научись распознавать мошеннические звонки

Очень распространены различные мошеннические звонки, например, мошенники представляются полицией, банком или курьерской службой.

В большинстве случаев целью мошенников является **украсть данные твоего аккаунта или кредитной карты.**

Запомни!

1. **Сотрудники банка и полиции не запрашивают твою информацию по телефону. Также не принимай предложение совершить за тебя транзакции и войти в твой компьютер по сети с помощью какой-либо программы.**
2. Если есть сомнения, прекрати разговор.
3. ПИН-коды твоей ID- карты предназначены только для тебя.

Сообщи о киберинциденте
cert@cert.ee

Больше информации
www.itvaatlik.ee