ПАМЯТКА КЛИЕНТАМ
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПРИ РАБОТЕ С СИСТЕМОЙ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ, КОТОРАЯ ПОМОЖЕТ ВАМ БЕЗОПАСНЕЕ РАБОТАТЬ В ИНТЕРНЕТЕ

Защита компьютера от вредоносного кода и хакерских атак

Слово "хакер" раньше использовался для обозначения высококвалифицированных программистов. Теперь так называют тех, кто использует уязвимости в программном обеспечении для внедрения в компьютерную систему. Это электронный эквивалент взлома помещения. Хакеры постоянно взламывают как отдельные компьютеры, так и крупные сети. Получив доступ к системе, они крадут конфиденциальные данные или устанавливают вредоносные программы.

Что такое уязвимость?

Современные приложения чрезвычайно сложны. Они компилируются из тысяч строк кода, но создаются они людьми, а людям свойственно ошибаться. Поэтому нет ничего удивительного в том, что в программы закрадываются ошибки, что делает их уязвимыми для атаки. Хакерам эти лазейки позволяют проникнуть в систему, а вирусописатели используют ошибки в коде приложений, чтобы обеспечить автоматический запуск на компьютере вредоносных программ.

Хакеры – это киберпреступники, которые проникают в вашу компьютерную систему, как в дом или квартиру, используя особые лазейки - уязвимости в программном обеспечении. Защититься от них можно с помощью установки на компьютер антивируса, регулярных обновлений операционной системы и офисных программ, в которых разработчики закрывают известные уязвимости, а также сетевого экрана. Сетевой экран, или файервол, при правильной настройке распознает попытки взлома и значительно затрудняет действия хакеров.

Не используйте компьютер предназначенный для работы с системой дистанционного банковского обслуживания для скачивания, установки и работы нелицензионного программного обеспечения, торрент-трекеров, программ для предоставления удаленного доступа или «анонимайзеров» - особых программ позволяющих получить доступ к запрещенным ресурсам в сети Интернет. Помните, что зачастую нелицензионное программное обеспечение содержит код хакеров, позволяющий обойти системы защиты и получить доступ к конфиденциальной информации. Если на предназначенном для работы в системе дистанционного банковского обслуживания компьютере операционная система, пакет офисных программ, браузер для доступа в Интернет или антивирус устарели и сняты с поддержки (не выпускаются обновления от разработчиков), его нельзя использовать для доступа к дистанционному банковскому обслуживанию.

Что такое «Мошенническое ПО»?

Большинство вредоносных программ, используемых для совершения преступлений – это разного рода троянские программы, или трояны. Одни из них регистрируют последовательность нажимаемых на клавиатуре клавиш, другие делают снимки экрана при посещении пользователем сайтов, предлагающих банковские услуги, третьи загружают на компьютер дополнительный вредоносный код, предоставляют хакеру удаленный доступ к компьютеру и т.д. Все эти программы объединяет то, что они позволяют злоумышленникам собирать конфиденциальную информацию и использовать ее для кражи денег у пользователей.

Как защитить компьютер от вредоносного кода и хакерских атак?

Вы сможете защитить свой компьютер от вредоносного кода и хакерских атак, если будете следовать приведенным ниже **несложным правилам**:

- Установите на своем компьютере решение для защиты от информационных угроз.

- Всегда устанавливайте обновления операционной системы и прикладных программ, предназначенные для устранения пробелов в их безопасности. Если вы пользуетесь Microsoft® Windows®, вам не нужно вручную загружать обновления каждый месяц, достаточно установить режим автоматических обновлений – Пуск | Панель управления | Центр обеспечения безопасности Windows® (Start | Control Panel | Security Center). Для Microsoft® Windows 10 ®, Пуск | Параметры | Центр обновления Windows® Если вы пользуетесь программным пакетом Microsoft® Office®, не забывайте регулярно устанавливать его обновления.
-  Если вы получили по электронной почте сообщение с вложенным файлом (документ Word, таблица Excel, исполняемый файл с расширением .EXE и т.д.), не открывайте вложение, если отправитель письма вам неизвестен. Не открывайте вложение и не переходите по ссылкам,если вы не ожидали получить подобное сообщение. НИ ПРИ КАКИХ УСЛОВИЯХ не открывайте вложения, присланные в нежелательных сообщениях (спаме).
- Регулярно (не реже раза в день) устанавливайте обновления программ, обеспечивающих безопасность вашего компьютера.
- Используйте на своем компьютере учетную запись с правами администратора только в тех случаях, когда вам надо установить программы или изменить настройки системы. Для повседневного использования создайте отдельную учетную запись с ограниченными правами пользователя (для этого нужно зайти в раздел "Учетные записи пользователей" Панели управления, для Microsoft® Windows 10 ®, Пуск | Параметры | Учетные записи). Это важно потому, что при атаке вредоносный код получает тот же уровень прав, с которым вы вошли в систему. Если вы зарегистрировались в системе с правами администратора, то такой же уровень прав будет и у вируса, червя или троянской программы, и вредоносное ПО получит доступ к ключевым данным, хранящимся в системе.
- Регулярно сохраняйте резервные копии своих данных на компакт-диске (CD), DVD-диске или внешнем USB-накопителе. В случае повреждения или шифрования вредоносной программой данных на жестком диске вы сможете восстановить их из резервной копии.

Для защиты от вредоносного кода и хакерских атак:

- Установите программу для обеспечения интернет-безопасности.
- Всегда устанавливайте обновления, отвечающие за безопасность.
- Будьте осторожны со спамом в электронной почте и системах мгновенных сообщений.
- Пользуйтесь учетной записью администратора на своем компьютере только в случае необходимости.
- Сохраняйте резервные копии данных.

Защита паролем.

Почему важны пароли для ваших учетных записей в интернете? Как выбрать надежный пароль

Сейчас у всемирной компьютерной сети пользователей больше, чем когда-либо ранее. Возможности ее использования также значительно расширились и включают электронные банковские услуги, онлайн-покупки и исследования, проводимые с помощью интернет-ресурсов.

К сожалению, чем больше пользователи работают и общаются в сети, тем выше риск кражи паролей и ЭП, используя которые в дальнейшем мошенническим путем крадут деньги непосредственно с банковских счетов своих жертв.

Поскольку пароли защищают конфиденциальную информацию, их важность трудно переоценить. Все ваши учетные записи в интернете должны быть защищены паролями. Но выбирать пароль нужно осмотрительно.

Пароль защищает ваши персональные и конфиденциальные данные от кражи, в том числе не позволяет злоумышленникам получить доступ к банковскому счету или другим электронным учетным записям и украсть ваши деньги.

Надежный пароль снижает риск стать жертвой киберпреступников. Наши **рекомендации** помогут вам создать пароли для ваших учетных записей в интернете.

Выбор надежного пароля

- Выбирайте пароли, которые вам будет легко запомнить и не придется записывать (в том числе вносить в файл на вашем компьютере). Такой файл может быть стерт, поврежден или украден киберпреступниками.
- Не используйте в качестве пароля реальные слова, которые киберпреступники могут найти в словаре. Используйте буквы как нижнего, так и верхнего регистра, а также цифры и другие символы – например, знаки препинания (хотя использование последних не всегда разрешено).
- Не прибегайте к "ротации" паролей, когда "пароль1", "пароль2", "пароль3" и т.д. используются попеременно для разных учетных записей.
- Если возможно, используйте в качестве пароля словосочетание, а не отдельное слово.
- Не используйте один и тот же пароль для разных учетных записей. В противном случае, подобрав только один пароль, злоумышленники получат доступ ко всем вашим онлайн-аккаунтам.

Пароль – это секрет

- Не используйте для защиты своих данных очевидные пароли, которые легко угадать: имя вашего супруга (супруги), ребенка, домашнего животного, номера телефонов, регистрационный номер машины, почтовый индекс и т.п.
- Не сообщайте никому свой пароль. Если с вами связался (например, по телефону) представитель некой организации и попросил сообщить ваш пароль, не раскрывайте свои личные данные: вы не знаете, кто на самом деле находится на другом конце провода.
- Не записывайте логин и пароль на бумаге
- Не используйте функцию запоминания логина и пароля в браузерах;
- Не вводите логин и пароль Интернет-банка на компьютерах, которые находятся в общедоступных местах (например, интернет кафе).
- Регулярно меняйте пароли.
- Не используйте одинаковые логин и пароль для доступа к различным системам.
- Если онлайн-магазин или веб-сайт прислал вам по электронной почте сообщение с подтверждением регистрационной информации и новым паролем, как можно скорее зайдите на соответствующий сайт и смените пароль.
- Убедитесь в том, что установленное на вашем компьютере программное обеспечение для защиты от интернет-угроз блокирует попытки перехвата или кражи.