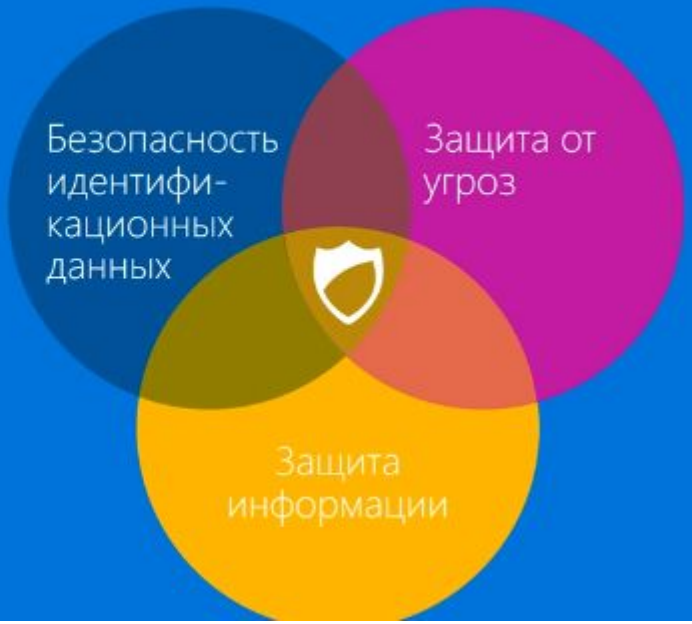
Windows 10
Безопасность



Безопасность в Windows 10

- Безопасность идентификационных данных
  - Credential Guard
  - Windows Hello
  - Microsoft Passport
- Защита информации
  - Enterprise Data Protection (EDP)
  - BitLocker
  - Encrypting File System (EFS)
- Защита от угроз
  - Device Guard

Device Guard в действии

Демонстрация

Device Guard

Что такое Device Guard?

- Комбинация аппаратных и программных средств обеспечения безопасности
- Возможность для организации строго контролировать, запуск каких приложений разрешен на устройстве
- Реализация на десктопных компьютерах режима работы, схожего с поведением ОС на мобильных устройствах, например, Windows Phone

Device Guard

Компоненты решения

- Безопасность на аппаратном уровне
- Безопасность на основе виртуализации (Virtualization based security, VBS)
  - Защита критических компонент ОС от вредоносного кода, запущенного на уровне ядра
- Настраиваемая проверка целостности кода (Code Integrity, CI)
- Инструменты управления: GP, SCCM, MDM, PowerShell

Проверка целостности кода (CI)

- Secure Boot
  - Включая Secure Firmware Updates и Platform Secure Boot
- Kernel Mode Code Integrity (KMCI)
- User Mode Code Integrity (UMCI)
- AppLocker

Что такое Malware (малварь) и как с этим бороться?

Malware или «Малварь», сокращенно от английского «malicious software» - вредоносное программное обеспечение, имеющее своей целью в той или иной форме нанести ущерб пользователю или компьютеру и его содержимому. Малварь - общее название для всех видов кибер-угроз, таких как: вирусы, трояны, шпионские программы, кейлоггеры, adware и др. Malware или вредоносы - достаточно распространенный вид кибер-угроз, и столкнуться с вредоносным ПО может каждый.

Spyware (**шпионское программное обеспечение**, **программа-шпион**) — программа, которая скрытным образом устанавливается на компьютер, смартфон, персональный цифровой помощник с целью сбора информации о конфигурации компьютера, копировании информации из памяти устройства, копировании данных пользователя, аудио/видео записи пользователя или пользовательской активности без согласия последнего. Также могут производить другие действия: изменение настроек, установка программ без ведома пользователя, перенаправление действий пользователя. В настоящий момент существует множество определений и толкований термина

Adware (англ.; от *ad*, *advertisement* — «реклама» и *software* — «программное обеспечение» = **рекламное программное обеспечение**, **рекламная программа**) — тип лицензирования программного обеспечения. Само программное обеспечение распространяется бесплатно, однако автор или распространитель приложения получает доход за счет показа рекламы.

Также, термином «adware» называют тип зловредной программы, которая навязчивым образом отображает нежелательные объявления.

Что такое scareware?

Scareware - это разновидность вредоносных программ, которые используют тактику запугивания, чтобы заставить вас сделать покупку и установку вредоносного ПО. Обычно она появляется в виде агрессивного всплывающего окна или баннера, на котором отображается фальшивое сканирование на вирусы, указывающее на то, что ваша система находится в серьезной опасности. Затем она предлагает вам купить или установить какую-нибудь зараженную антивирусную программу, чтобы немедленно "решить" эту проблему. Конечно, предложенный антивирус только ухудшит ситуацию.

browser hijacker - форма нежелательного программного обеспечения, которое изменяет настройки веб-браузера без разрешения пользователя». Результатом является размещение нежелательной рекламы в браузере и, возможно, замена существующей домашней страницы или страницы поиска

Потенциально нежелательная программа (ПНП) или потенциально нежелательные приложения (НСД) является программным обеспечением , которое пользователь может воспринимать как нежелательные.

Такое программное обеспечение может использовать реализацию, которая может поставить под угрозу конфиденциальность или ослабить безопасность компьютера. Компании часто связывают желаемую загрузку программы с приложением-оберткой и могут предложить установить нежелательное приложение, а в некоторых случаях и без предоставления явного способа отказа.

ФИШИНГ

Фи́шинг (англ. *phishing* от *fishing* «рыбная ловля, выуживание»[1]) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Subdomains & Misspelt

http://www.google.com.stationx.net

http://stationx.net/sa/google.com/support/

http://www.rnicrosoft.com

IDN homograph attack

http://www.g00gle.com

http://www.goog1e.com

Hidden URLs

Click Here

https://www.google.com/