Информационная безопасность на период работы из дома

Апрель 2020

pwc

Содержание

- Социальная инженерия
- Фишинговые письма
- Вредоносные программы
- Кража паролей
- Утечка конфиденциальной информации
- Безопасность в сети Интернет
- Порча корпоративного имущества
- Режим работы

Социальная инженерия

Социальная инженерия - это различного рода манипулирование людьми с целью получения конфиденциальной информации. При этом злоумышленники могут попытаться выведать информацию как при непосредственном общении с целью, так и убедить цель использовать зловредное программное обеспечение. Для противодействия социальной инженерии, мы рекомендуем соблюдать следующие меры безопасности:

Никогда и никому не сообщайте личные и конфиденциальные данные (пароли, ПИН-коды, номера банковской карты, коды от SMS подтверждения и т.д). Будьте предельно осторожны с людьми, которые представляются сотрудниками служб поддержки и просят предоставить им подобную информацию.

Не подключайте к компьютеру носители информации, кроме тех, которые должны использоваться в соответствии с установленными в организации бизнес-процессами.

Не используйте корпоративные носители информации (флешки, переносные диски и т.п) при работе с личными устройствами, так как зловредное программное обеспечение может перейти с личного устройства на носитель и, в дальнейшем, на корпоративные устройства.

Более подробную информацию о различных видах социальной инженерии можно получить из соответствующих общедоступных материалов в Интернете.

Фишинговые письма

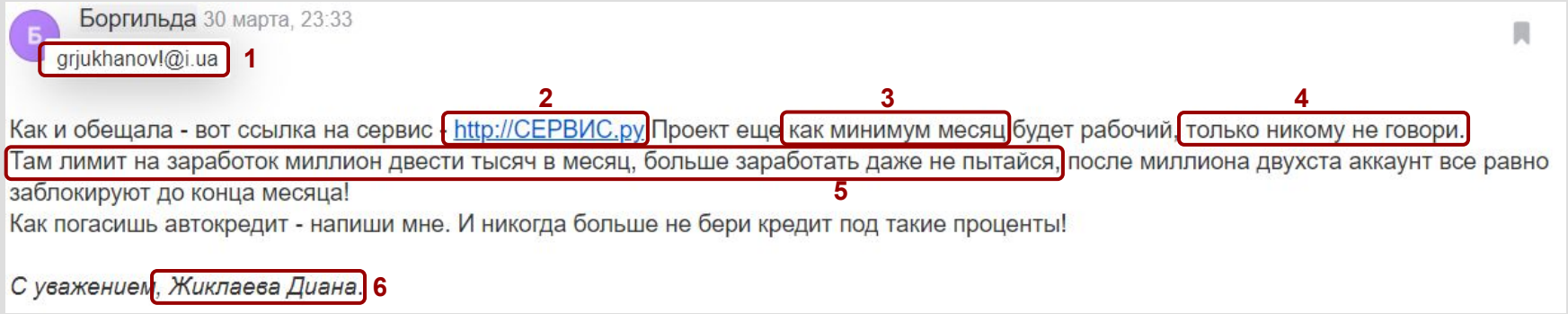
Фишинг - это разновидность социальной инженерии с использованием фальшивых электронных писем или веб сайтов, которые злоумышленники выдают за подлинные. Целью фишинга является получение конфиденциальной информации (учетных записей, данных банковских карт и счетов и т.п.). Пользователи электронной почты и Интернета стали более подвержены фишинговым атакам из-за повышенного использования этих ресурсов во время COVID-19. Чтобы снизить риски, связанные с фишинговыми атаками, мы рекомендуем соблюдать следующие меры безопасности:

При получении письма с ссылкой на какой-либо внешний источник, который не является официальным порталом организации, необходимо проверить, куда ведет данная ссылка, или же подтвердить у отправителя, что это он направил письмо с данной ссылкой.

Если письмо направил незнакомый адресат, то не рекомендуется переходить по ссылкам в письме и скачивать вложения, особенно если это файлы с расширением .zip, .rar, .7z, .exe, .src, .dll, .sys, .bat, .js, .vbs, .js, .mht, .cmd, .xlsm.

Необходимо связаться и проинформировать службу ИТ или отдел информационной безопасности организации при обнаружении частых фишинговых атак.

Пример того, как выглядит фишинговое письмо



1) Сложный для чтения адрес: мошенники, как правило, используют сгенерированный случайным образом набор символов в качестве адреса отправителя
2) Ссылка, куда рекомендуют перейти, не является защищенным сайтом, т.к. отсутствует индикатор HTTPS
3) Настаивают на том, чтобы пользователь как можно скорее перешел по ссылке
4) Просят никому не сообщать, входя в доверие: ведь информация якобы только “для своих”
5) Устанавливают ограничения, чтобы войти в доверие, но при этом ставя ограничение в значительную сумму
6) ФИО в подписи никак не сходится ни с адресом ящика, откуда пришло письмо, ни с именем почты
Более подробную информацию о различных видах фишинговых атак можно получить из соответствующих общедоступных материалов в Интернете.

Вредоносные программы

Вредоносные программы создаются специально для несанкционированного пользователем уничтожения, блокирования, изменения или копирования информации, нарушения работы компьютеров, или компьютерных сетей. Чтобы избежать риска “заражения” компьютера подобной программой, мы рекомендуем соблюдать следующие меры безопасности:

- Не отключать и не ограничивать работу функционирования систем безопасности устройства (файрволл, антивирус). Не отключать автоматическое обновление системы/приложений.

- Работать на компьютере исключительно под правами пользователя, а не администратора, что в значительной мере предотвратит установку вредоносного программного обеспечения и изменение системных настроек без ведома пользователя.

- В период удаленной работы крайне важно ограничить доступ к устройству, с которого осуществляется рабочий процесс: установить пароль на учетную запись, ограничить физический доступ к устройству.

- Если работа осуществляется с устройства, к которому имеют доступ дети, то рекомендуется создать для них отдельную учетную запись и ограничить возможность установки программ/игры, а также закрыть доступ к папкам с рабочими файлами.

- Устанавливать только лицензионное программное обеспечение. Не запускать неизвестные файлы, особенно с расширением .zip, .rar, .7z, .exe, .src, .dll, .sys, .bat, .js, .vbs, .js, .mht, .cmd, .xlsm, .docm.

Кража паролей

Пароль - это набор символов, который используется для защиты доступа к учетной записи пользователя. Пароли являются ценной информацией для злоумышленников. Чтобы снизить риск кражи паролей, мы рекомендуем соблюдать следующие меры безопасности:

- Создавать сложные пароли (от 8 символов, содержащие буквы (заглавные и строчные), цифры, спец.символы (! # $ и т.п.)). Не использовать функционал автоматического заполнения паролей.

- Не переходить по подозрительным ссылкам (например - ссылки, предоставленные в чатах WhatsApp, которые ведут на непроверенные источники).

- При получении информации о необходимости смены пароля от какого-либо сервиса не затягивать со сменой пароля. Не использовать одинаковые пароли для различных сервисов.

- Если есть возможность, использовать двухфакторную аутентификацию для всех сервисов, которыми пользуетесь: когда вход на портал осуществляется не только с помощью одного пароля, но и дополнительного кода, например - с помощью одноразовых пин-кодов по смс.

- Регулярно менять пароли (1 раз в 2-3 месяца), регулярно проверять наличие учетных записей в соответствующих базах скомпрометированных учетных записей, доступных в Интернете, не использовать скомпрометированный (взломанный и опубликованный) ранее пароль.

Утечка конфиденциальной информации

В процессе удаленной работы, появляются новые риски, связанные с потенциальной угрозой утечки конфиденциальной информации. Чтобы снизить риск утечки информации, мы рекомендуем соблюдать следующие меры безопасности:

Не открывать конфиденциальные файлы/почту на некорпоративном устройстве, обеспечить защиту устройства от вирусов (установить последние доступные обновления операционной системы и антивирусного программного обеспечения).

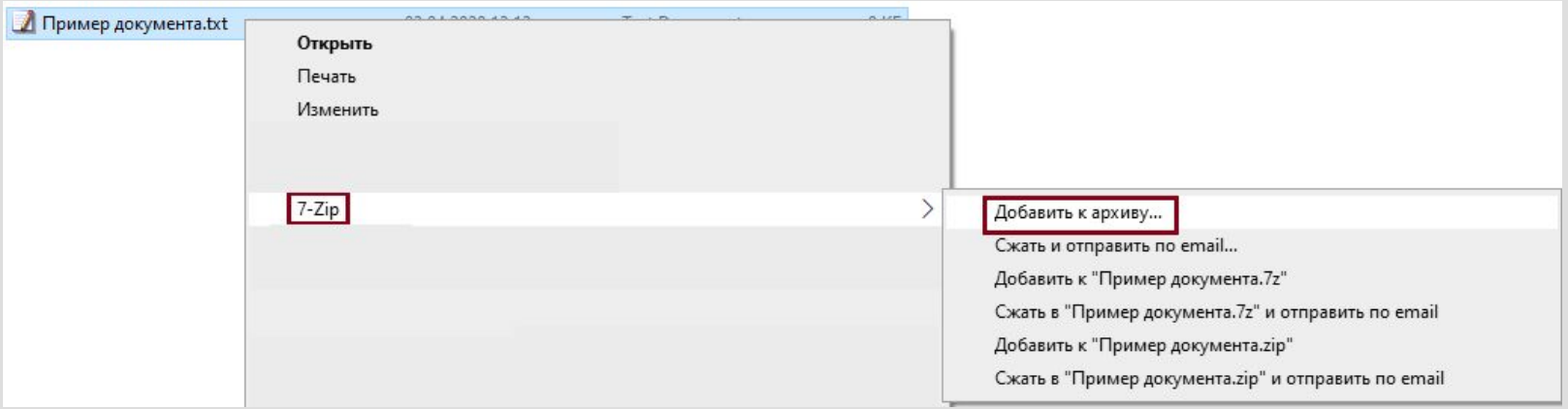
При обмене информацией с другими сотрудниками/клиентами - шифровать файлы с помощью архиваторов, при этом устанавливая сложный к подбору пароль, который должен быть передан по отдельному каналу связи, например, отдельным письмом. Алгоритм шифрования файла с помощью архиватора 7-Zip, показан на слайдах 9-10.

При распечатке дома каких-либо документов, необходимо удостовериться, что никто посторонний не имеет доступа к этим документам. Хранить документы следует в защищенном месте, например, в запираемом шкафу, к которому есть доступ только у вас.

Если документ более не нужен или был распечатан по ошибке, то его необходимо уничтожить безопасным образом: если имеется шредер для бумаги, то использовать его; если имеется корпоративный шредер в офисе, то сложить документы отдельно, в безопасном месте, и после появления возможности попасть в офис, отвезти и уничтожить в офисе; при неимении другой возможности - мелко измельчить документ своими силами и утилизировать, желательно - в разные пакеты для мусора.

Алгоритм архивации документов на примере 7 - Zip

Шаг 1.

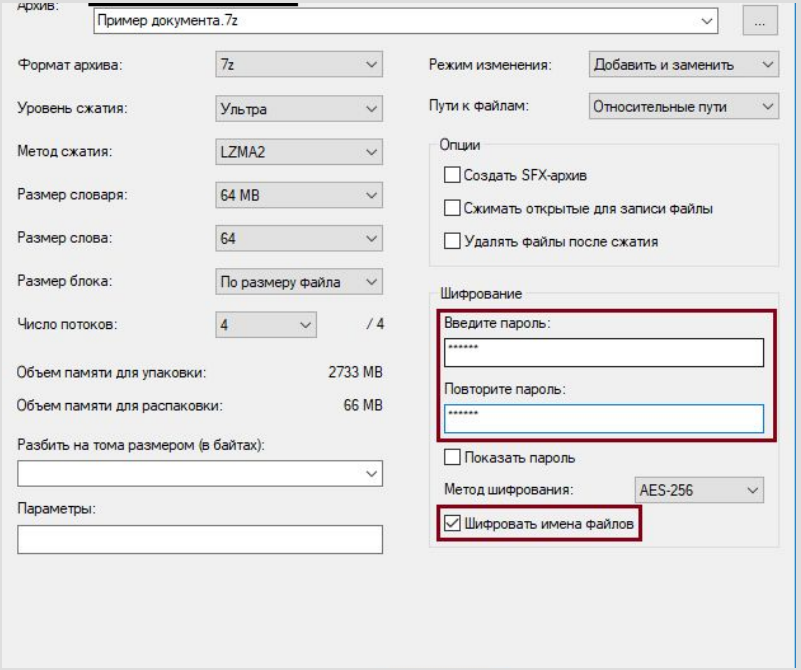


Для того, чтобы заархивировать папку (либо набор файлов и каталогов) достаточно кликнуть по ней правой кнопкой мыши и выбрать из выпадающего контекстного меню пункты «7-Zip» — «Добавить к архиву».

Алгоритм архивации документов на примере 7 - Zip

Шаг 2.

В результате вы увидите окно настроек архивирования, где помимо других настроек сможете задать пароль для доступа к этому архиву, а точнее зашифровать все содержимое папки (одновременно его архивируя), а данный пароль будет являться ключом к расшифровке.
Также необходимо отметить опцию “Шифровать имена файлов”, чтобы без ввода пароля невозможно было увидеть содержимое архива.



Безопасность в сети Интернет

Так как удаленный режим работы подразумевает активное использование сети Интернет, следует уделить особое внимание безопасности во время его использования. Как это сделать, описано ниже:

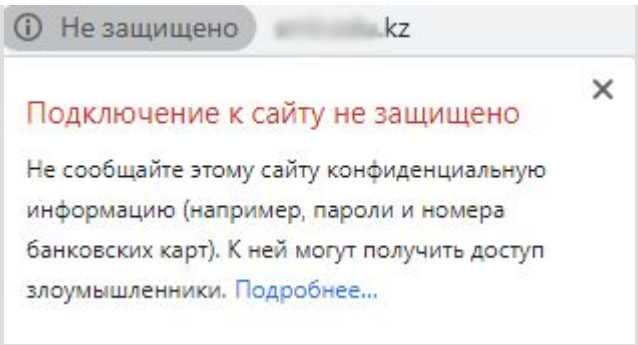
Не игнорируйте предупреждения веб-браузера или антивируса о плохо защищенном сайте. Не посещайте те сайты, у которых нет сертификатов безопасности. Индикатором наличия сертификата безопасности является соответствующий значок в адресной строке и начало адреса с HTTPS. Примеры безопасного и небезопасного соединения можно увидеть на слайде 12.

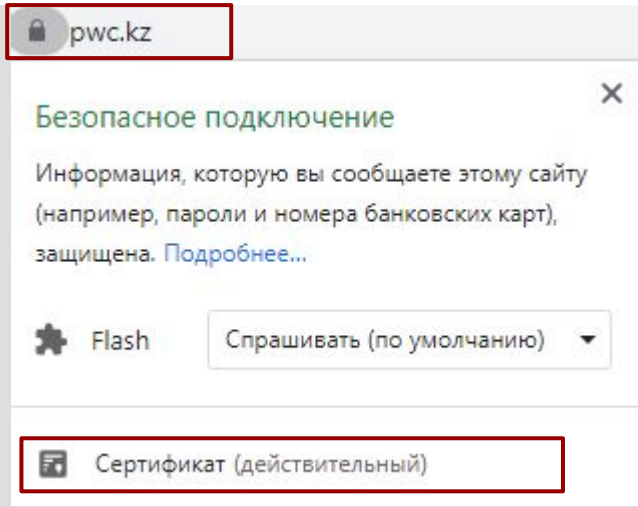
При наличии возможности подключения к корпоративной сети через VPN, при каждом использовании устройства проверяйте наличие успешного подключения.

Не доверяйте непроверенным Wi-Fi-соединениям, которые не запрашивают пароль. Чаще всего именно такие сети злоумышленники используют для воровства личных данных пользователей. О том, как проверить используемое подключение, можно посмотреть на слайдах 13-14.

Рекомендуем настраивать сложный пароль для домашней беспроводной сети и выбирать более сложный алгоритм защиты Wi-Fi сети (WPA2).Подробнее о том, как правильно настроить Wi-Fi на роутере, можно посмотреть на сайте производителя устройства.

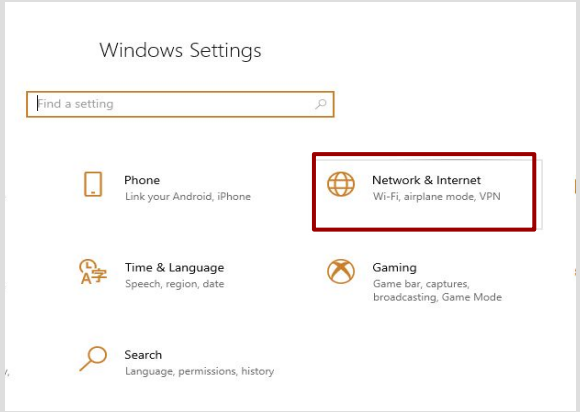
Пример того, как выглядит небезопасное и безопасное соединение в браузере Google Chrome

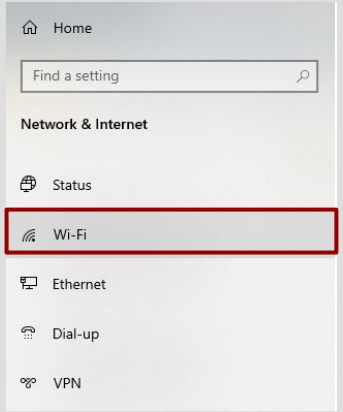


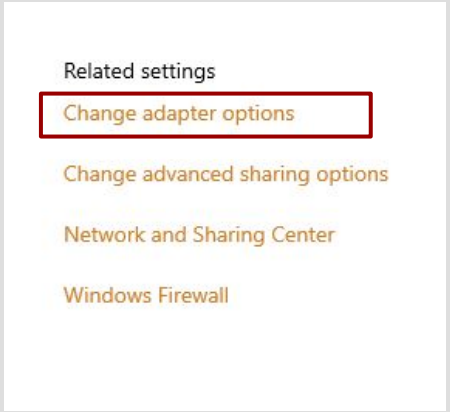


Сертификаты, которые проверяются специальными организациями или системами и имеют подтверждение что их сформировал реальный владелец сайта. И еще одним элементов безопасности сайта является расширенный протокол HTTPS.

Как узнать тип безопасности WiFi на ПК?

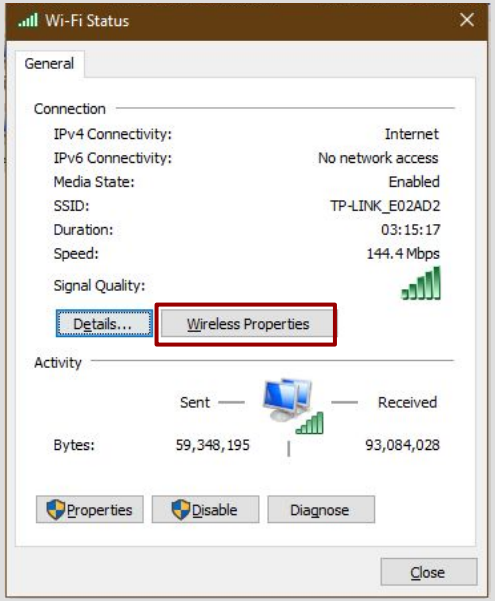


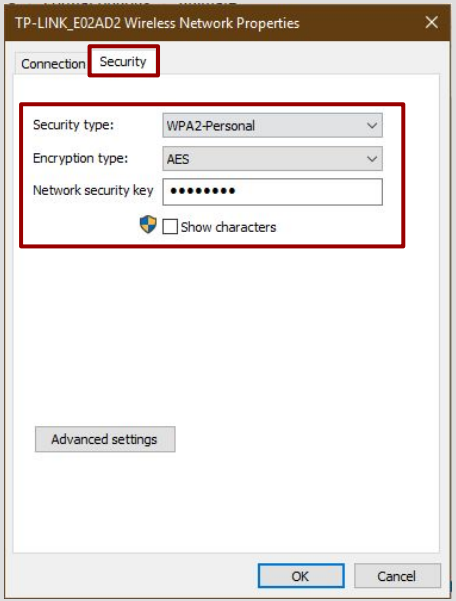




Для начала необходимо зайти в панель Настройки, затем выбрать Сети и Интернет. Далее вкладку WiFi, и на этой вкладке надо будет выбрать Изменить опции адаптера.

Как узнать тип безопасности WiFi на ПК? (*продолжение*)





После этого на экране появляется окно Сетевые соединения, там выбираем WiFi. Уже здесь, мы видим Состояние Беспроводной сети. И выбираем Свойства беспроводной сети. Во вкладке Безопасность мы рекомендуем настраивать сложный пароль и выбирать WPA2 как тип безопасности.

Порча корпоративного имущества

В связи с введением карантина, доступ к IT-поддержке ограничен, поэтому следует предельно бережно относиться к корпоративным устройствам, с которыми вы работаете. Зачастую замена ноутбука или дополнительного устройства невозможна в условиях карантина. Наши рекомендации по защите вашего рабочего устройства представлены ниже:

Ответственно относитесь к имуществу компании.

Не оставляйте рабочее устройство под солнцем или во влажном помещении.

Будьте предельно аккуратными с любыми жидкостями вблизи рабочего устройства.

Не занимайтесь приемом пищи при работе за компьютером.

Апрель, 2020

Режим работы

Усталость от переработки может значительно снизить внимание и привести к несоблюдение мер информационной безопасности. Мы рекомендуем следующие простые меры по эффективной работе из дома:

Распределите время для работы, приема пищи и отдыха, соблюдайте выбранный режим.

При работе с компьютером периодически разминайтесь и делайте зарядку для глаз.

Спасибо

pwc.com

© 2020 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.