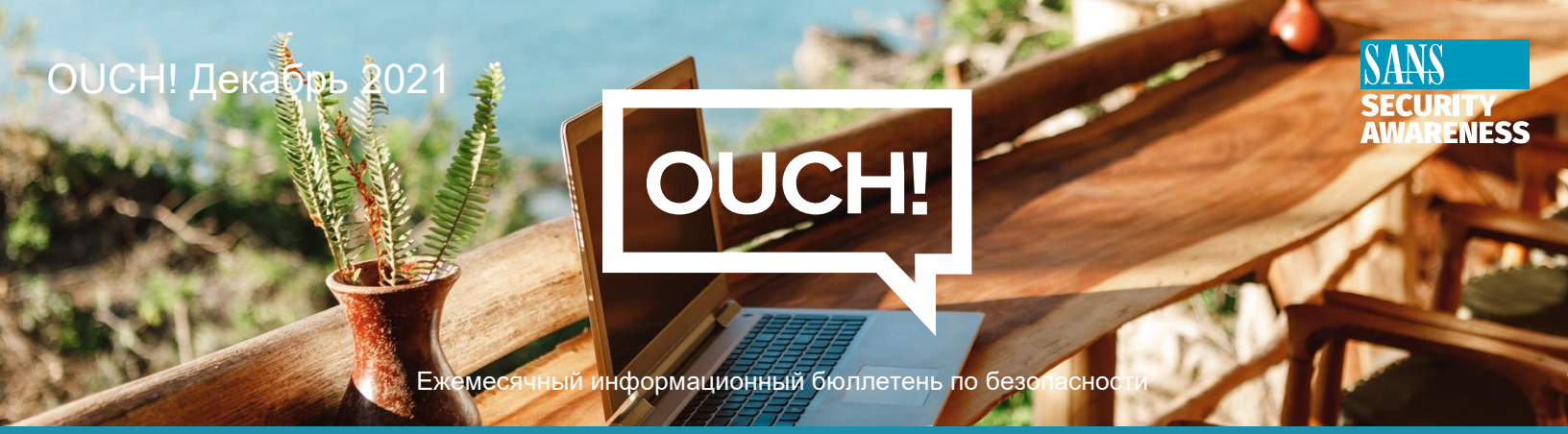

Ежемесячный информационный бюллетень по безопасности

Советы по кибербезопасности во время отпуска

Обзор

По мере приближения курортного сезона миллионы людей будут путешествовать. Если вы один из них, вот несколько советов, которые помогут вам оставаться в безопасности в киберпространстве.

- **Мобильные устройства**: возьмите с собой как можно меньше устройств. Чем меньше устройств вы возьмете с собой в поездку, тем меньше вероятности что вы их потеряете или у вас их украдут. На самом деле, знаете ли вы, что у вас гораздо больше шансов потерять мобильное устройство, чем его украдут? Каждый раз, покидая гостиничный номер, ресторан, такси, поезд или самолет, сделайте быструю проверку и убедитесь, что вы ничего не забыли. Если с вами путешествуют друзья или семья, дважды проверьте чтобы ничего не забыть, например, дети, которые могут оставить устройство на сиденье или в ресторане.

  Что касается устройств, которые вы решили взять с собой, обязательно обновите их, чтобы на них была установлена последняя версия операционной системы и приложений. Не отключайте блокировку экрана. Если возможно, убедитесь, что у вас есть способ удаленно отслеживать ваши устройства в случае их потери. Кроме того, вам может потребоваться возможность удаленного стирания данных с устройства. Таким образом, если устройство потеряно или украдено, вы можете удаленно отслеживать или стирать все ваши конфиденциальные данные и учетные записи. Наконец, сделайте резервную копию со всех устройств, которые вы берете с собой, чтобы в случае потери или кражи вы могли легко восстановить свои данные.

- **Подключения Wi-Fi**: Во время путешествия вам может потребоваться подключение к общедоступной сети Wi-Fi. Имейте в виду, что вы не знаете, кто настроил эту сеть Wi-Fi, кто и как ее отслеживает и кто еще к ней подключен. Вместо того, чтобы подключаться к общедоступной сети Wi-Fi, по возможности подключайтесь к персональной точке доступа вашего смартфона и используйте ее. Таким образом, вы знаете, что у вас есть надежное соединение Wi-Fi. Если это невозможно и вам необходимо подключиться к общедоступной сети Wi-Fi (например, в аэропорту, отеле или кафе), используйте виртуальную частную сеть, часто называемую VPN. Это программное обеспечение, которое вы устанавливаете на свой ноутбук или мобильные устройства, чтобы защитить и анонимизировать ваше соединение Wi-Fi. Некоторые решения VPN включают настройки для автоматического включения VPN при подключении к ненадежным сетям Wi-Fi.

- **Общественные компьютеры**: избегайте использования общедоступных компьютеров, например, в вестибюлях отелей или в кафе, для входа в какие-либо учетные записи или доступа к конфиденциальной информации. Вы не знаете, кто использовал этот компьютер до вас, и возможно, они случайно или намеренно заразили его вредоносным ПО, например регистратором нажатия клавиш. Придерживайтесь устройств, которые вы контролируете и которым доверяете.

- **Социальные сети**: мы любим сообщать другим о наших путешествиях и приключениях через социальные сети, но мы не всегда знаем, кто за нами наблюдает в сети. По возможности избегайте чрезмерного обмена информацией во время отпуска и подумайте о том, чтобы подождать, пока вы не вернетесь домой, чтобы поделиться своей поездкой. Кроме того, не размещайте фотографии посадочных талонов, водительских прав или паспортов, поскольку это может привести к краже личных данных.

- **Работа**: если вы будете работать во время отпуска (мы надеемся, что нет!), Убедитесь, что вы заранее проверили, какие правила в отношении ваших рабочих поездок, в том числе, какие устройства или данные вы можете взять с собой и как безопасно удаленно подключаться к рабочим системам.

Отпуск должен быть временем для расслабления, изучения и веселья. Эти простые шаги помогут вам сделать это безопасно и надежно.

Приглашенный редактор

Принцесса Янг является старшим аналитиком Southwest Airlines и руководит работой по обучению в области кибербезопасности 60 000 сотрудников по всей стране. Принцесса любит взаимодействовать с сотрудниками, чтобы они чувствовали себя вправе разделить ответственность за кибербезопасность, независимо от их роли или звания.

Ресурсы

Защита ваших мобильных устройств: https://www.sans.org/newsletters/ouch/securing-mobile-devices/
Сила обновления: https://www.sans.org/newsletters/ouch/the-power-of-updating/
Виртуальные частные сети: https://www.sans.org/newsletters/ouch/Virtual-Private-Networks/
Резервные копии: https://www.sans.org/newsletters/ouch/got-backups/

Роман Полаков