CYBER READINESS
INSTITUTE

Праздничный сезон начинается! Как быть киберзащищенным в праздники

Во время сезона праздников как компании, так и покупатели подвергаются риску кибератак. Многие правительственные организации, в том числе ФБР, Агентство безопасности критически важной инфраструктуры (CISA) и Национальный центр кибербезопасности Великобритании, выпустили рекомендации о том, как лучше всего оставаться в безопасности в течение праздничного сезона. Институт киберготовности (CRI) собрал главное из этих уведомлений в путеводитель из двух частей на период праздников для покупателей и розничных продавцов.

Покупатели

Имейте в виду, что хакеры всегда ищут наиболее эффективные способы связаться с вами.

Согласно отчету, опубликованному Proofpoint, праздничный фишинг (или смишинг) с помощью текстовых сообщений (SMS) почти удвоился по сравнению с прошлым годом.

Хакеры отправляют сообщения с помощью текстовых сообщений и электронных писем, имитируя доставку.

Лучшие практики

- ☑ Проверьте свои устройства: используйте надежные пароли или парольные фразы длиной не менее 15 символов, обновите программное обеспечение и включите многофакторную аутентификацию.
- ☑ Покупайте только через проверенные источники: подумайте о том, как и где вы совершаете покупки в Интернете.
- ☑ Распознавайте фишинговые схемы: не переходите по ссылкам и не загружайте вложения, если не уверены, откуда они пришли. Дважды проверьте адрес эл. почты отправителя и будьте осторожны с запросами личной информации.
- ☑ Никогда не сообщайте свой пароль, личную или финансовую информацию в ответ на нежелательное эл. письмо или телефонный звонок.
- ☑ Используйте безопасные способы для покупок: никогда не предоставляйте финансовую информацию при использовании общедоступного Wi-Fi.

Продавцы

Это самое загруженное время года не только для вас, но и для хакеров.

Остерегайтесь атак программ-вымогателей. В 2020 году многие известные компании пострадали во время праздников в США, когда злоумышленники знали, что компании будут изо всех сил пытаться выполнить заказы.

Sophos Labs подсчитала, что в 2020 году розничная торговля была наиболее пострадавшим сектором от кибератак.

Источники:

[illegible]?utm_camping=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202 https://www.politico.com/newsletters/national-security-daily/2021/11/22/chinas-missile-turducken-495192 https://us-cert.cisa.gov/ncas/current-activity/2021/11/22/reminder-critical-infrastructure-stay-vigilant-against-threats https://www.cisa.gov/news/2021/11/22/cisa-and-fbi-urge-organizations-remain-vigilant-ransomware-and-cyber-threats https://www.proofpoint.com/us/blog/corporate-news/holiday-shopping-themed-mobile-attacks-increase-dramatically https://us-cert.cisa.gov/ncas/alerts/aa21-243a https://www.washingtonpost.com/politics/2021/11/24/happy-hacksgiving-officials-warn-surge-cyber-threats/

Лучшие практики:

- Определите специалистов по технологиям и кибербезопасности, которые могут быстро от- реагировать в праздничные дни, если произойдет киберинцидент.
- Предупредите сотрудников о том, что в праздничные дни следует опасаться фишинговых писем и других кибермошенников.
- Убедитесь, что обновления ПО установлены на всех устройствах компании и на всех личных устройствах, используемых вашим персоналом для выполнения своей работы.
- Обязательно используйте надежные пароли, гарантируя, что они не используются повторно в нескольких аккаунтах.
- Убедитесь, что каждая компьютерная система требует, чтобы пользователи использовали многофакторную аутентификацию, особенно для удаленного доступа и административных учетных записей.
- Напомните сотрудникам не нажимать на подозрительные ссылки и проводите тренинги для повышения осведомленности.
- Просмотрите и, при необходимости, обновите планы реагирования на инциденты и планы коммуникации, чтобы перечислить действия, которые организация предпримет в случае воздействия инцидента.
- Убедитесь, что ваши важные системы и данные защищены резервными копиями в месте, которое не подключено к вашей сети.

Помните:

Если вы стали жертвой кибератаки, сообщите об инциденте в службу кибербезопасности вашего правительства.

На becyberready.com, cisa.gov/shop-safely, us-cert.cisa.gov/ncas/alerts/aa21-243a и stopransomware.gov вы получите дополнительную информацию и рекомендаций о том, как оставаться в безопасности в этот праздничный сезон.

CYBER READINESS INSTITUTE