По материалам НЦПТИ (Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет)

«Безопасная Сеть»: Как защититься от мошенничества и травли в интернете

В издательстве «Альпина Паблишер» вышла книга «Безопасная Сеть: Правила сохранения репутации в эпоху социальных медиа и тотальной публичности». Ее автор — писатель и профессор бизнес-школы Эрик Куалман, известный своими работами о цифровой экономике и социальных медиа. The Village публикует советы из книги о том, как избежать проблем в интернете.

7 советов по защите личных данных

- Помните: ваш смартфон уязвим. Убедитесь, что на ваших компьютерах, мобильных устройствах и переносных гаджетах установлены последние программные средства защиты. Почаще обновляйте это программное обеспечение.

- Не пользуйтесь публичным Wi-Fi для финансовых операций. Если вы пользуетесь публичным Wi-Fi в гостинице или ресторане, не проводите банковских операций, операций с акциями или других важных финансовых транзакций. Занимайтесь ими в безопасности, дома.
- Остерегайтесь бесплатного Wi-Fi. Преступники, занимающиеся кражей личных данных, часто называют точки доступа к Wi-Fi официальными именами различных мест, в том числе гостиниц, аэропортов или ресторанов. Например, точка доступа может называться «freewifi» или «hotelwifi». Если вы пользуетесь этими незащищенными сетями, вы рискуете. Если вы не уверены, какой Wi-Fi официальный, просто спросите служащего аэропорта, администратора гостиницы или официанта.

- Избегайте фишинг-мошенничества. В случае получения по электронной почте писем от компаний, банков или других организаций не переходите по ссылкам. Гораздо безопаснее зайти напрямую на страницы этих сайтов и найти конкретное предложение или вопрос. Если вы все-таки решите перейти по ссылке, убедитесь, что URL правильный. Например, www.bankofamerica.com, а не bankofamerica.randomsite.com. Мошенники создают поддельные сайты и поддельные мейлы, притворяясь известными компаниями. Так у мошенников появляется возможность украсть ваш пароль и личную информацию.

- Не публикуйте важную личную информацию в социальных сетях. Выбирайте секретные контрольные вопросы, на которые невозможно ответить с помощью информации, размещенной на вашей странице в Facebook. Используйте сложные пароли для всех своих учетных записей.

➢ Используйте сложные пароли, включающие в себя символы, цифры и буквы в верхнем и нижнем регистре, для защиты ваших личных данных. Если вам в голову ничего не приходит, попробуйте метод мнемоники. Например, «Я родился в нью-йоркской больнице Мерси в 1975 году» превращается в «Яр@н-йбМв1975г». Используйте разные пароли, потому что ворам легче получить доступ к вашей личной информации, когда вы используете один и тот же пароль для своих учетных записей.

➢ Храните подтверждение заказа. Завершив покупки онлайн, вы увидите страницу подтверждения, на которой перечислены позиции вашего заказа и указана информация о клиенте, продукте и номер подтверждения. Распечатайте экземпляр страницы подтверждения, а также страницу с указанием названия компании, ее почтового адреса, номера телефона и юридические условия, включая политику возврата. Храните эти распечатки в течение гарантийного периода / периода возврата. Продавец также может отправить вам по электронной почте сообщение с подтверждением заказа. Сохраните и/или распечатайте это сообщение, как любую другую переписку с компаниями.

10 советов о том, как обезопасить себя и свою семью в интернете

- Не публикуйте фотографии ваших детей с подписанными именами.
- Не публикуйте даты отъезда в отпуск и возвращения домой.
- Защищайте свой Wi-Fi и устанавливайте на него пароль.
- Не публикуйте фотографии, на которых видны номера вашей машины, адрес и другая личная информация.
- Не пишите полностью свое имя, адрес или дату рождения в публичных профилях. Чем меньше вы напишете, тем лучше.
- Не публикуйте материалы, из которых понятен ваш ежедневный график или привычки.
- Практикуйте безопасную работу в интернете и используйте только защищенные сайты. Проверяйте наличие «https://» при пользовании кредитной картой. «S» означает «защищенный» (secure).
- ОЧЕНЬ внимательно читайте политику конфиденциальности. Большинство сайтов пишут, как они используют вашу информацию.
- Настаивайте, чтобы ваши дети пользовались никами, когда играют на интерактивных игровых приставках вроде Xbox Live, Nintendo и т. д. Используйте родительский контроль для защиты ваших детей.
- Обсудите со своими детьми потенциальные опасности интернета. Пусть ваш диалог будет открытым.

6 советов тем, кто стал жертвой кибертравли

- Обратитесь за помощью к тем, кому вы доверяете.
- Не удаляйте оскорбительные сообщения. Вы можете не читать их, но храните в качестве доказательства.
- Не отвечайте на оскорбления. Ваши ответы раззадоривают агрессоров и дают им чувство значимости и влияния.
- Заблокируйте отправителя оскорбительных сообщений.
- Сообщите о проблеме вашему интернет-провайдеру, администрации сайта и в полицию.
- Вы не можете контролировать действия тех, кто вас травит, но вы можете контролировать свою реакцию. Если они смогут вывести вас из себя, они победили.