Russian

Обеспечьте защиту ваших персональных данных

Каждый год в США девять миллионов человек становятся жертвами кражи персональных данных. Для обеспечения защиты своих персональных данных соблюдайте следующие важные правила:

1 Обеспечьте защиту личной информации

- **Не отвечайте на подозрительные предложения, поступающие по телефону, по почте, в виде СМС и по электронной почте.** Не передавайте свои персональные данные по телефону, по электронной почте, СМС, а также на сайтах социальных сетей. Никогда не переходите на незнакомые ссылки, получаемые по электронной почте, даже если они поступают из источников, которым вы доверяете; это могут быть «фишинг-мошенники», маскирующиеся под надежные источники, с тем чтобы «выудить» у вас личную информацию. Помните о том, что адреса электронной почты и телефонные номера могут оказаться поддельными, чтобы выглядеть так, как будто сообщение поступило от вашего знакомого.
- **Обеспечьте защиту своего компьютера, планшета, смартфона от вирусов и «вредоносных программ» с помощью программных средств антивирусной и сетевой защиты.** Не вводите свои персональные данные, когда пользуетесь незащищенной сетью Wi-Fi, создавайте надежные личные пароли, загружайте программное обеспечение и прикладные программы исключительно из тех источников, которым вы доверяете. Не следует сообщать слишком много личной информации о себе на сайтах социальных сетей, будьте осторожны при пользовании программными средствами геотегирования. Зайдите на сайт **OnGuardOnline.gov**, чтобы получить более подробную информацию о том, как лучше всего обеспечить безопасность личных данных в онлайновом режиме.
- **Будьте очень осторожны, пользуясь общедоступными компьютерами.** Перед выходом из системы удалите все документы личного характера и очистите «корзину». Проверьте интернет-настройки и убедитесь в том, что компьютер удаляет все сведения из истории просмотра. При использовании общедоступного компьютера никогда не совершайте какие-либо онлайновые покупки при помощи своей кредитной или платежной карты.
- **Ежегодно проверяйте свою кредитную историю.** Один из способов проверки, не стали ли вы жертвой кражи персональных данных, — бесплатная загрузка вашей кредитной истории с сайта **annualcreditreport.com**.
- **Ограничьте количество карточек, которые вы с собой носите.** Оставьте при себе только те кредитные или платежные карты, которыми вы планируете воспользоваться, а остальные храните в надежном месте. Никогда не носите с собой карточку социального обеспечения.

2 Контролируйте свою почту

- **Необходимо знать, когда обычно приходят ежемесячные счета на оплату и отчеты о состоянии вашего банковского счета.** Следите за их своевременным поступлением. Подпишитесь на получение отчетности по электронной почте и оплату счетов в онлайновом режиме, чтобы предотвратить риск кражи персональных данных из почты.
- **Следите за необычными операциями в выписках с банковских счетов и отчетах по кредитным картам.** Даже беглая проверка позволит своевременно выявить существующую проблему.
- **Отправляясь в отпуск, приостановите доставку почты.** Посетите сайт **usps.com/holdmail** или позвоните по телефону **1-800-275-8777**, чтобы передать запрос о приостановлении доставки почты.

3 Будьте осторожны, совершая покупки

- **Проверяйте квитанции.** Убедитесь в том, что в квитанциях не указана дата окончания срока действия вашей кредитной карты и отсутствует ее полный номер, за исключением последних пяти цифр. В соответствии с законами г. Нью-Йорка это требование относится ко всем коммерческим предприятиям.
- **При совершении покупки следите за своей кредитной картой.** Известны случаи, когда сотрудники пользовались портативными приспособлениями для незаконного считывания информации с карточек для последующих хакерских операций со счетами клиентов.

4 Пользуйтесь устройствами для измельчения бумаги

- **Все под нож!** Вместо того чтобы просто выбрасывать ненужные бумаги, лучше использовать приспособления для их измельчения, особенно в том случае, когда они содержат персональные данные, такие как:

  ✔ номер социального обеспечения;
  ✔ номера банковских счетов или кредитных карт;
  ✔ информацию о паролях или PIN-кодах;
  ✔ дату рождения;
  ✔ конфиденциальные контактные данные;
  ✔ подпись.

- **Перейдите на электронные документы.** Перейдите на электронную отчетность и по возможности производите оплату в режиме онлайн.

5 Вы полагаете, что стали жертвой кражи персональных данных? Примите неотложные меры!

- **Закройте все счета, которые были мошенническим путем открыты от вашего имени.** Свяжитесь с отделами по борьбе с мошенничеством в каждой компании, где от вашего имени обманным путем были открыты счета или произведены покупки, которые вы не совершали.
- **Поставьте в известность компетентные органы.** Сообщите о краже персональных данных в местный полицейский участок и отправьте соответствующее заявление в Федеральную торговую комиссию на сайте **ftc.gov/idtheft** или по телефону **1-877-ID-THEFT** (1-877-438-4338). Сохраните копии вашего обращения и заявления.
- **Предупредите о возможных фактах мошенничества одно из трех агентств кредитной истории: Equifax, Experian, TransUnion**. Будучи предупреждены о возможном мошенничестве относительно вашей кредитной истории, кредиторы должны связаться с вами перед тем как открыть новый счет или внести какие-либо изменения в существующие счета. Тщательно документируйте всю переписку.
- **Вы можете получить бесплатные индивидуальные консультации по финансовым вопросам.** Зайдите на сайт **nyc.gov/TalkMoney** или позвоните по телефону **311** и попросите дать вам адрес ближайшего Центра финансовой поддержки г. Нью-Йорка. Консультанты помогут вам разобраться с финансовыми вопросами, вызывающими у вас затруднения.

NYC Consumer and Worker Protection

Более подробную информацию можно найти по сайте nyc.gov/dcwp.