Обеспечение кибербезопасности при работе со служебными сведениями

1. Для обмена служебной информацией необходимо использовать только **служебные (корпоративные) адреса** электронной почты.
2. Необходимо обращать внимание на электронные письма, содержащие подозрительную информацию. **Это может быть фишинг**.

Фишинг представляет собой сетевой вид мошенничества, при котором технически подкованные мошенники выманивают у людей конфиденциальную информацию. Главная задача фишинга — получение логина и пароля пользователя для определённого сайта, с дальнейшим их использованием. Это могут быть идентификационные данные вашего банковского кабинета или ПИН-код с номером карточки для вывода на свой счёт ваших денег. Часто фишинг используют для доступа к аккаунтам в социальных сетях. В любом случае, когда ваш логин и пароль становятся известны злоумышленникам, последствия для вас будут весьма удручающие.

Чтобы не стать жертвой подобного вида мошенничества необходимо:

- сверять адреса электронной почты организации и ее контактные данные с официальными источниками;

- не переходить по незнакомым ссылкам из писем, не открывать подозрительные вложения;

- получив подозрительное сообщение от друга/коллеги, необходимо связаться с ним и убедиться, что он действительно его отправлял;

- не звоните по указанному в подозрительном письме номеру телефона и не вступайте в переписку;

- используйте последние версии интернет-браузеров и лицензионные антивирусные программы;

- при входе на банковские сайты следите за тем, чтобы было установлено защищённое соединение https.

3. Необходимо **установить надежные пароли** на всех своих устройствах, включить отслеживание их по GPS и не оставлять без присмотра;

© 2024 Следственное управление Следственного комитета Российской Федерации по Республике Татарстан

4. **Недопустимо копировать информацию**, содержащую охраняемую законом тайну, на личные устройства и съемные носители.

5. Распечатанные документы **необходимо забирать сразу** после окончания печати.

6. Документы на бумажных и электронных носителях, **содержащие конфиденциальные сведения**, необходимо всегда держать под присмотром, а в случае отсутствия на рабочем, месте **запирать в сейф**.

7. Ненужные документы, содержащие **конфиденциальные сведения** необходимо **уничтожать с помощью шредера.**

Основы защита банковских карт от мошенничества

1. Не сообщайте никому данные своей банковской карты, номер самой карты или счета, и что важнее, трехзначный код, расположенный на оборотной стороне карты (CVV), и не передавайте SMS-коды неизвестным людям.
2. Опасайтесь стать жертвой социальной инженерии. Это явление один из самых распространенных способов мошенничества с банковскими картами. Если Вам поступает звонок от лица, представившегося сотрудником правоохранительных органов и сообщает, что кто-либо из ваших близких совершил правонарушение и для «благополучного решения вопроса» необходимо перечислить N-ю сумму денег с вашей банковской карты, обязательно свяжитесь с человеком, которого пытаетесь спасти.
3. Никогда не устанавливайте неофициальные версии мобильных приложений, не пользуйтесь сомнительными приложениями и регулярно обновляйте антивирусы на своих смартфонах и планшетах.
4. Не доверяйте сомнительным сообщениям о блокировке вашей банковской карты с предложением сообщить сувои персональные данные, PIN-код и т.п. Никто не имеет права узнавать у вас такую информацию, даже сотрудники банка, выпустившего вашу карту.
5. Никогда не передавайте людям вашу банковскую карту. Если кто-то другой попытается оплатить с помощью данных вашей банковской карты свои покупки, на номер телефона, который связан с вашей картой должен прийти одноразовый код, игнорируйте его и никому не сообщайте.
6. Никогда не пишите PIN-код карты на самой карте и не храните его вместе с картой.
7. Не выбрасывайте в урну чек, который распечатывает банкомат, так как на нем может быть напечатана информация с логинами и паролями для входа в онлайн-банкинг.

© 2024 Следственное управление Следственного комитета Российской Федерации по Республике Татарстан

Соблюдение этих несложных правил позволит вам не стать жертвой мошенников!

Адрес страницы: https://tatarstan.sledcom.ru/folder/1792648/item/1792676

© 2024 Следственное управление Следственного комитета Российской Федерации по Республике Татарстан