Главе администрации
МР Благовещенский район РБ

Главам сельских поселений
МР Благовещенский район

# ПАМЯТКА ПО ЗАЩИТЕ ОТ КИБЕРМОШЕННИКОВ

Межрайонная Благовещенская прокуратура направляет правила самозащиты от кибермошенников:

- К своей основной карте в вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее.

- Регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций. Подключите SMS-оповещение об операциях по карте. С его помощью можно сразу увидеть, если злоумышленник совершит по ней операцию, заблокировать карту и опротестовать операцию.

- Храните номер карточки и ПИН–коды в тайне. Запомните и сотрите/заклейте CVC-код, не сообщайте коды даже сотрудникам банков. Реальный сотрудник банка никогда не будет их у вас спрашивать.

- Используйте виртуальные карты, которые сейчас предоставляют платежные системы.

- Поставьте лимит на сумму списаний или перевода в личном кабинете банка.

- Будьте осмотрительны в отношении писем со вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных вам отправителей и всегда проверяйте вложения на наличие вирусов.

- Не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма. Мошенники создают сайт, имитирующий официальный сайт банка, а затем рассылают письма от лица кредитной организации на электронную почту клиента. По прямой ссылке он переходит на поддельный сайт: как правило, такой сайт идентичен официальному сайту банка, а доменное имя отличается буквой или символом. После того, как клиент вводит личные данные, в том числе информацию о карте, CVC и пин-код, с его карты списываются деньги.

Не заполняйте полученные по электронной почте формы и анкеты. Личные данные можно вводить лишь на защищенных сайтах. Мошенники в электронных письмах или на фейковых аккаунтах в соцсетях от имени крупных компаний предлагают пройти опрос. За ответы на несколько простых вопросов пользователю обещают от нескольких десятков до нескольких сотен тысяч рублей. Чтобы получить деньги, нужно перевести незначительную сумму. После того, как средства оказываются у мошенников, последние исчезают.

- Проверяйте запросы персональных данных из деловых и финансовых структур. Лучше обратиться в эти структуры по контактам, указанным на официальном сайте, а не в электронном письме.
- Насторожитесь, если кроме вас в электронном сообщении указаны другие адресаты. Маловероятно, что при общении с клиентом по поводу личных учетных данных банк использует многоадресную рассылку.
- Насторожитесь, если от вас требуют немедленных действий или представляется чрезвычайная ситуация. В данном случае преступники вызывают у вас ощущение тревоги, чтобы заставить вас действовать быстро и неосмотрительно.
- Старайтесь не афишировать личные данные, содержащие даты рождения, адреса электронной почты или имена домашних животных, которые могут использоваться как пароли.
- Остерегайтесь сообщений подобного рода: «Внимание! Ваш аккаунт был взломан. Вы должны позвонить, чтобы подтвердить свой аккаунт. Отправьте нам сообщение, и мы перезвоним Вам».
- Точки Wi-Fi чаще всего небезопасны, так как не кодируют информацию, передаваемую в интернете. Более того, инструменты, которыми пользуются хакеры, позволяют им выудить имена пользователей, пароли или другую информацию, предоставляющую доступ к финансовым счетам.
- Не используйте одинаковый пароль для разных учётных записей. Выбирайте для паролей необычные символы, цифры и пробелы. В качестве дополнительной меры предосторожности, заполните вопросы безопасности вымышленными, простыми для запоминания ответами, а не фактами, которые могли бы раскрыть ваши личные данные.
- Установите на компьютер антивирусное и антишпионское программное обеспечение. Убедитесь, что эти программы работают и обновляются автоматически.
- Не устанавливайте неизвестные приложения. Иногда мошенники просто просят свою жертву установить на телефон программу, а потом зайти в

интернет-банк. После этого злоумышленник получает доступ к денежным средствам.

- Не переводите деньги незнакомцам и даже знакомым если Вас об этом просят, так как профиль человека может быть взломан.
- Если вам звонят из банка, уточните ФИО и должность сотрудника и скажите, что перезвоните ему сами. Номер нужно набрать вручную. В случае сомнения в достоверности истории, рассказанной Вам сотрудником банка, кладите трубку и перезванивайте сами на горячую линию своего банка».
- Внимательно изучайте сообщение от банка (e-mail или SMS). Если адрес электронной почты или номер отправителя вызывают сомнения или сообщение не внушает доверия — обращайтесь за дополнительной информацией в круглосуточный call-центр банка (номер указан на официальном сайте и на вашей карте). Не переходите по прямой ссылке и не перезванивайте на номер отправителя SMS.

Межрайонный прокурор
советник юстиции Д.С. Елизаров