Чтоб не оказаться жертвой мошенников

ВАЖНО ЗНАТЬ

- сотрудники банка при телефонном разговоре не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты);
- храните пин-код отдельно от карты, не пишите пин-код на самой банковской карте, не сообщайте пин-код третьим лицам;
- избегайте телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка или правоохранительных органов, лучше прервать разговор;
- не сообщайте пароли и секретные коды, которые приходят Вам в СМС-сообщении;
- действуйте обдуманно, не торопливо, свяжитесь со службой поддержки своего банка, узнайте, все ли в порядке с Вашей картой;

- не покупайте в интернет-магазинах или сайтах-объявлениях товары по явно заниженной стоимости – это очевидно мошенники;
- не переводите денежные средства, если об этом вас просит сделать Ваш знакомый в социальной сети, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком, узнайте действительно ли он просит у Вас деньги;
- не переходите в сети «Интернет» по ссылкам на неизвестные сайты;
- не совершайте сомнительные переводы денежных средств на счета незнакомых или малознакомых лиц, предлагающих Вам на различных сайтах товар или услуги.

ПРОКУРАТУРА ХАБАРОВСКОГО РАЙОНА РАЗЪЯСНЯЕТ

2025

«Как не стать жертвой преступлений, совершаемых в сети «Интернет»

Сегодня и взрослые, и молодые люди являются активными пользователями Интернет-сети. С развитием современных информационных технологий, увеличивается и количество нарушений закона с использованием информационно-телекоммуникационных технологий, так называемых киберпреступлений, в том числе и с участием несовершеннолетних (кража денежных средств, кража персональных данных, распространение незаконного интернет-контента, кибер-издевательства, сбыт наркотических средств, распространения порнографических материалов с привлечением несовершеннолетнего и т.д.).

Злоумышленники используют разные способы обмана людей в интернете от спама до создания сайтов-двойников.

Они преследуют ЦЕЛЬ - получить персональные данные пользователя, номера банковских карт, паспортные данные, логины и пароли.

У потерпевших похищаются денежные средства под предлогом совершения каких-либо банковских операций, направленных на восстановление якобы поврежденных данных о банковских вкладах, либо путем введения их в заблуждение.

При этом зачастую злоумышленники представляются банковскими работниками или представителями правоохранительных органов.

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ ВИДЫ МОШЕННИЧЕСТВ В «ИНТЕРНЕТЕ» ВЫРАЖАЮТСЯ В:

- приобретении товаров и услуг посредством сети «Интернет»;
- призывах о помощи;
- звонках от родственника, попавшего в беду;
- звонках от работника банка (представителя службы безопасности);
- звонках от сотрудника полиции (следственного комитета, прокуратуры);
- приобретении товаров на сайтах объявлений (Авито и т.д.), заказах доставки чего-либо через сервисы «Блаблакар»;
- звонках от банковской организации с роботизированным текстом и другие.

Если Вам звонят и просят ответить на вопросы фразами «да» или «нет», то есть вероятность того, что в это время происходит взлом вашего банковского счета при помощи голосового управления.

Хабаровский край, г. Хабаровск,
ул. Краснореченская, д. 70А
Адрес электронной почты:
hbrn.phk@181.mailop.ru

г. Хабаровск
2025 год