

Приложение 1 к письму Отделения-  
НБ Карачаево-Черкесская Республика  
«О направлении материалов по  
киберграмотности»

*Ссылка и QR-код на информационные видеоролики Банка России по теме профилактики кибермошенничества:*

<https://disk.yandex.ru/d/MEwy-ZliXds1KA;>



1. Аналитические данные Банка России за 2023 год -

[http://www.cbr.ru/analytics/ib/operations\\_survey/2023/;](http://www.cbr.ru/analytics/ib/operations_survey/2023/)



2. Ежеквартальная статистика Банка России -

[http://www.cbr.ru/statistics/ib/#a\\_118726;](http://www.cbr.ru/statistics/ib/#a_118726;)



3. Ссылка на образовательные материалы, в составе которых  
«конструктор» слайдов –

[https://finclass.info/\\_wt/cybergram;](https://finclass.info/_wt/cybergram;)



4. Карточки по тематике киберграмотности –

**Банк России**

## ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

**1 ЗАБЛОКИРОВАТЬ КАРТУ**  
 По номеру или номеру счета звоните в службу поддержки или на официальный сайт банка. Используйте мобильное приложение.

**2 НАПИСАТЬ ЗАЯВКУ НЕОСРОЧНО С ОПЕРАЦИЕЙ**  
 В течение 30 минут деньги будут списаны с вашей карты. Если вы не успеваете сделать это, обратитесь в отделение банка.

**3 ОБРАТИТЬСЯ В ПОЛИЦИЮ**  
 Если вы обнаружили кражу денег, немедленно сообщите об этом в полицию. Вам необходимо написать заявление.

**КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?**

**НИКОМУ НЕ СООБЩАЙТЕ:**  
 номер карты и срок ее действия, номер кода безопасности (CVV2/CVC2), PIN-код, номер счета, номер мобильного телефона.

**НЕ ПИШИТЕ ЗАЯВКИ:**  
 по электронной почте, по телефону, по факсу, по почте.

**ОСТАВЛЯЙТЕ:**  
 номер счета и номер мобильного телефона.

**Банк не гарантирует:**  
 защиту от краж денег с помощью средств безопасности.

**Финансовая культура**

**Банк России**

## ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

### 5 ПРИЗНАКОВ ОБМАНА

**1 НА ВАС ВЫХОДИТ САНИ**  
 Ассистент или помощник по телефону банка, страховой компании, полиции, налоговой, пенсионного фонда.

**2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУШАЮТ**  
 Сильные эмоции вызывают желание сообщить о выгоде.

**3 ГОВОРЯТ О ДЕНЬГАХ**  
 Говорят о выгоде, о возможности получить деньги, о возможности получить кредит.

**4 НА ВАС ДАВЯТ**  
 Ассистент или помощник по телефону банка, страховой компании, полиции, налоговой, пенсионного фонда.

**5 ПРОСИТ СООБЩИТЬ ДАННЫЕ**  
 Запрашивают номер мобильного телефона, номер карты, пароль и код из банка для подтверждения.

**ВАЖНО!**  
 Сотрудник банка и полиции НИКОГДА не спрашивают номер карты, пароли, PIN-код, номер счета, номер мобильного телефона и не просят сообщить персональные данные.

**НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:**  
 номер карты, номер мобильного телефона, номер счета, номер мобильного телефона, номер карты, пароль и код из банка для подтверждения, персональные данные.

**Финансовая культура**

**Банк России**

## КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг – это мошенничество, при котором злоумышленники пытаются получить доступ к вашим личным данным, номерам карт, паролям и другим важным данным.

**КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?**  
 При переходе по ссылке или по ссылке из SMS, электронной почты, сообщения в мессенджере, по телефону.

**КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?**  
 Адрес сайта не совпадает с адресом банка, в адресной строке не отображены логотипы банка, в адресной строке не отображены логотипы банка, в адресной строке не отображены логотипы банка.

**КАК УВЕРИТЬСЯ ОТ ФИШИНГА?**  
 Уточнить по телефону или по электронной почте номер счета, номер мобильного телефона, номер карты, номер счета, номер мобильного телефона.

**Финансовая культура**

**Банк России**

## КАК ЗАЩИТИТЬСЯ ОТ ОНЛАЙН-МОШЕННИКОВ

Чтобы добро пасть до ваших банковских счетов, мошенникам нужны ваши персональные данные и реквизиты карт.

**Какие схемы используют аферисты?**

**ОБМАНЧИВЫЕ ВОЗМОЖНОСТИ**  
 Обещают вернуть деньги, вернуть деньги, вернуть деньги.

**ВНЕЗАПНОСТЬ НА РАБОТНОМ МЕСТЕ**  
 Обещают вернуть деньги, вернуть деньги, вернуть деньги.

**ОБЪЕДИНЕНИЕ НА РАБОТНОМ МЕСТЕ**  
 Обещают вернуть деньги, вернуть деньги, вернуть деньги.

**КАК ОБЕЗОПАСИТЬ СВОИ ДЕНЬГИ В ИНТЕРНЕТЕ?**

1. Проверить адрес сайта и убедиться, что сайт принадлежит банку.
2. Проверить наличие логотипа банка и убедиться, что сайт принадлежит банку.
3. Проверить наличие логотипа банка и убедиться, что сайт принадлежит банку.
4. Не сообщать персональные данные и номер карты.
5. Не сообщать персональные данные и номер карты.

**Финансовая культура**