



УМВД России по Сахалинской области

ФИШИНГОВЫЕ АТАКИ

сообщает

ФИШИНГ

Обход фильтров
вид фишинга, который
использует
изображение вместо текста,
что затрудняет обнаружение
мошеннических электронных
писем антифишинговыми
фильтрами

Социальная
инженерия
вид фишинга, который
своими действиями
заставляет встревожить
пользователя и вызвать
у него немедленную
реакцию

Неправомерная деятельность, направленная на преступное
присвоение доступа к конфиденциальным данным
пользователей, таким, как логины, пароли, данные пластиковых
банковских карт и др.

Смишинг
(SMS фишинг)
вид фишинга, который
направлен на рассылку
сообщений, содержащих
ссылку на фишинговый
сайт

Веб-ссылки
вид фишинга, который
призван замаскировать
подделанные ссылки на
фишинговые сайты под
ссылки настоящих
организаций

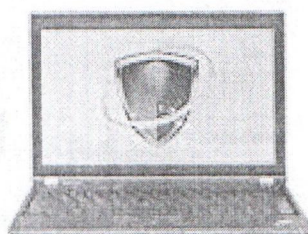
Веб-сайты
вид фишинга, который
использует JavaScript
для изменения
адресной строки

Вишинг
(голосовой фишинг)
вид фишинга, который
направлен на создание
сообщений на сайтах
для пользователей о
необходимости
позвонить по
определенному номеру
для решения проблем с
их банковскими счетами



Как уберечь себя от фишинга?

- Никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/CVVV2 код).
- Пользуйтесь только защищенными сайтами: https (где «s» означает «secure» - безопасное.)
- Не вносите какие-либо предоплаты за товар.
- Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети.
- Переходя на сайт банка проверяйте наличие защищенного входа (зеленая полоса перед строкой ссылки) и внимательно проверяйте внешний облик сайта.
- Не переходите по неизвестным ссылкам и не открывайте подозрительные электронные письма.
- Проверяйте адрес сайта, обращайте внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во всплывающей подсказке).
- Игнорируйте звонки и sms с неизвестных номеров и не заполняйте никакие формы в Интернете.



Всю информацию, поступившую посредством сети, обязательно проверяйте.

УМВД России по Сахалинской области

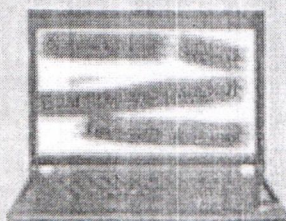
ОСТОРОЖНО МОШЕННИКИ!

ВНИМАНИЕ!
ФИШИНГОВЫЕ АТАКИ

Фишинг – новый вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другое. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например от имени банков, сервисов или внутри социальных сетей. В эти письма мошенники вставляют ссылки на фальшивые сайты, являющиеся точной копией настоящих.

Чем опасны сайты-подделки?

- крадут пароли
- распространяют вредоносные ПО
- навязывают платные услуги



Как уберечь себя от мошенников?

- Никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/CVVV2 код, номер карты и дату окончания срока действия).
- Пользуйтесь только защищенными сайтами: https (где «s» означает «secure» - безопасное.)
- Не вносите какие-либо предоплаты за товар, чтобы для вас его зарезервировали и не продали другому лицу, за возможное трудоустройство, а также в качестве аванса за сдачу жилья в наем.
- Оплачивайте товар по возможности при личной встрече и после проверки.
- Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети.
- Переходя на сайт банка проверяйте наличие защищенного входа (зеленая полоса перед строкой ссылки).
- Внимательно проверяйте внешний облик сайта.
- Не переходите по неизвестным ссылкам и не открывайте подозрительные электронные письма.
- Проверяйте адрес сайта, обращайте внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во всплывающей подсказке).
- Игнорируйте звонки и sms с неизвестных номеров и не заполняйте никакие формы в Интернете.



ПОМНИТЕ ВЫ МОЖЕТЕ СНИЗИТЬ УГРОЗУ ФИШИНГА, НЕМНОГО ИЗМЕНИВ СВОЕ ПОВЕДЕНИЕ



УМВД России по Сахалинской области

ФИШИНГОВЫЕ АТАКИ

сообщает

ФИШИНГ

Обход фильтров вид фишинга, который использует изображение вместо текста, что затрудняет обнаружение мошеннических электронных писем антифишинговыми фильтрами

Социальная инженерия

вид фишинга, который своими действиями заставляет встревожить пользователя и вызвать у него немедленную реакцию

Неправомерная деятельность, направленная на преступное присвоение доступа к конфиденциальным данным пользователей, таким, как логины, пароли, данные пластиковых банковских карт и др.

Смишинг

(SMS фишинг)

вид фишинга, который направлен на рассылку сообщений, содержащих ссылку на фишинговый сайт

Веб-ссылки

вид фишинга, который призван замаскировать подделанные ссылки на фишинговые сайты под ссылки настоящих организаций

Веб-сайты

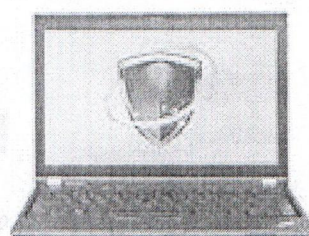
вид фишинга, который использует JavaScript для изменения адресной строки

Вишинг (голосовой фишинг) вид фишинга, который направлен на создание сообщений на сайтах для пользователей о необходимости позвонить по определенному номеру для решения проблем с их банковскими счетами



Как уберечь себя от фишинга?

- Никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/CVV2 код).
- Пользуйтесь только защищенными сайтами: https (где «s» означает «secure» - безопасное.)
- Не вносите какие-либо предоплаты за товар.
- Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети.
- Переходя на сайт банка проверяйте наличие защищенного входа (зеленая полоса перед строкой ссылки) и внимательно проверяйте внешний облик сайта.
- Не переходите по незнакомым ссылкам и не открывайте подозрительные электронные письма.
- Проверяйте адрес сайта, обращайте внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во всплывающей подсказке).
- Игнорируйте звонки и смс с незнакомых номеров и не заполняйте никакие формы в Интернете.



Всю информацию, поступившую посредством сети, обязательно проверяйте.

УМВД России по Сахалинской области

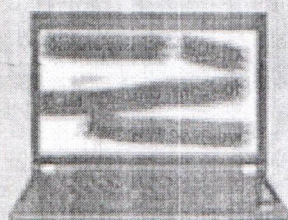
ВНИМАНИЕ!
фишинговые атаки

ОСТОРОЖНО МОШЕННИКИ!

ФИШИНГ – новый вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другое. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например от имени банков, сервисов или внутри социальных сетей. В эти письма мошенники вставляют ссылки на фальшивые сайты, являющиеся точной копией настоящих.

Чем опасны сайты-подделки?

- крадут пароли
- распространяют вредоносные ПО
- навязывают платные услуги



Как уберечь себя от мошенников?

- Никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/CVV2 код, номер карты и дату окончания срока действия).
- Пользуйтесь только защищенными сайтами: https (где «s» означает «secure» - безопасное.)
- Не вносите какие-либо предоплаты за товар, чтобы для вас его зарезервировали и не продали другому лицу, за возможное трудоустройство, а также в качестве аванса за сдачу жилья в наем.
- Оплачивайте товар по возможности при личной встрече и после проверки.
- Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети.
- Переходя на сайт банка проверяйте наличие защищенного входа (зеленая полоса перед строкой ссылки).
- Внимательно проверяйте внешний облик сайта.
- Не переходите по незнакомым ссылкам и не открывайте подозрительные электронные письма.
- Проверяйте адрес сайта, обращайте внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во всплывающей подсказке).
- Игнорируйте звонки и смс с незнакомых номеров и не заполняйте никакие формы в Интернете.



ПОМНИТЕ вы можете снизить угрозу фишинга, немного изменив свое поведение



УМВД России по Сахалинской области

ФИШИНГОВЫЕ АТАКИ
сообщает

ФИШИНГ

Обход фильтров вид фишинга, который использует изображение вместо текста, что затрудняет обнаружение мошеннических электронных писем антифишинговыми фильтрами

Социальная инженерия

вид фишинга, который своими действиями заставляет встревожить пользователя и вызвать у него немедленную реакцию

Неправомерная деятельность, направленная на преступное присвоение доступа к конфиденциальным данным пользователей, таким, как логины, пароли, данные пластиковых банковских карт и др.

Смишинг

(SMS фишинг) вид фишинга, который направлен на рассылку сообщений, содержащих ссылку на фишинговый сайт

Веб-ссылки

вид фишинга, который призван замаскировать подделанные ссылки на фишинговые сайты под ссылки настоящих организаций

Веб-сайты

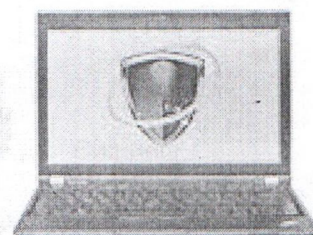
вид фишинга, который использует JavaScript для изменения адресной строки

Фишинг (голосовой фишинг) вид фишинга, который направлен на создание сообщений на сайтах для пользователей о необходимости позвонить по определенному номеру для решения проблем с их банковскими счетами

Как уберечь себя от фишинга?

- Никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/CVV2 код).
- Пользуйтесь только защищенными сайтами: https (где «s» означает «secure» - безопасное.)
- Не вносите какие-либо предоплаты за товар.
- Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети.
- Переходя на сайт банка проверяйте наличие защищенного входа (зеленая полоса перед строкой ссылки) и внимательно проверяйте внешний облик сайта.
- Не переходите по незнакомым ссылкам и не открывайте подозрительные электронные письма.
- Проверяйте адрес сайта, обращайте внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во всплывающей подсказке).
- Игнорируйте звонки и sms с незнакомых номеров и не заполняйте никакие формы в Интернете.

Всю информацию, поступившую посредством сети, обязательно проверяйте.



УМВД России по Сахалинской области

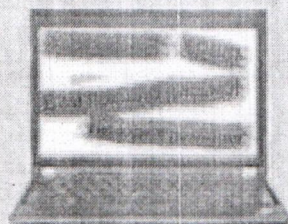
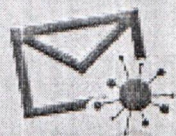
ОСТОРОЖНО МОШЕННИКИ!

ВНИМАНИЕ!
Фишинговые атаки

Фишинг – новый вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другое. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например от имени банков, сервисов или внутри социальных сетей. В эти письма мошенники вставляют ссылки на фальшивые сайты, являющиеся точной копией настоящих.

Чем опасны сайты-подделки?

- крадут пароли
- распространяют вредоносные ПО
- навязывают платные услуги

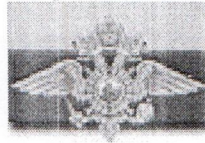


Как уберечь себя от мошенников?

- Никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/CVV2 код, номер карты и дату окончания срока действия).
- Пользуйтесь только защищенными сайтами: https (где «s» означает «secure» - безопасное.)
- Не вносите какие-либо предоплаты за товар, чтобы для вас его зарезервировали и не продали другому лицу, за возможное трудоустройство, а также в качестве аванса за сдачу жилья в наем.
- Оплачивайте товар по возможности при личной встрече и после проверки.
- Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети.
- Переходя на сайт банка проверяйте наличие защищенного входа (зеленая полоса перед строкой ссылки).
- Внимательно проверяйте внешний облик сайта.
- Не переходите по незнакомым ссылкам и не открывайте подозрительные электронные письма.
- Проверяйте адрес сайта, обращайте внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во всплывающей подсказке).
- Игнорируйте звонки и sms с незнакомых номеров и не заполняйте никакие формы в Интернете.



ПОМНИТЕ вы можете снизить угрозу фишинга, немного изменив свое поведение



УМВД России по Сахалинской области

сообщает

ФИШИНГ



Обход фильтров вид фишинга, который использует изображение вместо текста, что затрудняет обнаружение мошеннических электронных писем антифишинговыми фильтрами

Социальная инженерия вид фишинга, который своими действиями заставляет встревожить пользователя и вызвать у него немедленную реакцию

Неправомерная деятельность, направленная на преступное присвоение доступа к конфиденциальным данным пользователей, таким, как логины, пароли, данные пластиковых банковских карт и др.

Смишинг (SMS фишинг) вид фишинга, который направлен на рассылку сообщений, содержащих ссылку на фишинговый сайт

Веб-ссылки вид фишинга, который призван замаскировать подделанные ссылки на фишинговые сайты под ссылки настоящих организаций

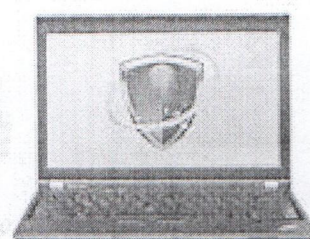
Веб-сайты вид фишинга, который использует JavaScript для изменения адресной строки

Вишинг (голосовой фишинг) вид фишинга, который направлен на создание сообщений на сайтах для пользователей о необходимости позвонить по определенному номеру для решения проблем с их банковскими счетами



Как уберечь себя от фишинга?

- Никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/CVVV2 код).
- Пользуйтесь только защищенными сайтами: https (где «s» означает «secure» - безопасное).
- Не вносите какие-либо предоплаты за товар.
- Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети.
- Переходя на сайт банка проверяйте наличие защищенного входа (зеленая полоса перед строкой ссылки) и внимательно проверяйте внешний облик сайта.
- Не переходите по незнакомым ссылкам и не открывайте подозрительные электронные письма.
- Проверяйте адрес сайта, обращайте внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во всплывающей подсказке).
- Игнорируйте звонки и смс с незнакомых номеров и не заполняйте никакие формы в Интернете.



Всю информацию, поступившую посредством сети, обязательно проверяйте.

УМВД России по Сахалинской области

ВНИМАНИЕ! ФИШИНГОВЫЕ АТАКИ

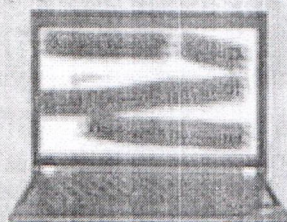
ОСТОРОЖНО МОШЕННИКИ!

ФИШИНГ – новый вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другое. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например от имени банков, сервисов или внутри социальных сетей. В эти письма мошенники вставляют ссылки на фальшивые сайты, являющиеся точной копией настоящих.



Чем опасны сайты-подделки?

- крадут пароли
- распространяют вредоносные ПО
- навязывают платные услуги



Как уберечь себя от мошенников?

- Никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/CVVV2 код, номер карты и дату окончания срока действия).
- Пользуйтесь только защищенными сайтами: https (где «s» означает «secure» - безопасное).
- Не вносите какие-либо предоплаты за товар, чтобы для вас его зарезервировали и не продали другому лицу, за возможное трудоустройство, а также в качестве аванса за сдачу жилья в наем.
- Оплачивайте товар по возможности при личной встрече и после проверки.
- Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети.
- Переходя на сайт банка проверяйте наличие защищенного входа (зеленая полоса перед строкой ссылки).
- Внимательно проверяйте внешний облик сайта.
- Не переходите по незнакомым ссылкам и не открывайте подозрительные электронные письма.
- Проверяйте адрес сайта, обращайте внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во всплывающей подсказке).
- Игнорируйте звонки и смс с незнакомых номеров и не заполняйте никакие формы в Интернете.



ПОМНИТЕ вы можете снизить угрозу фишинга, немного изменив свое поведение



УМВД России по Сахалинской области

сообщает

ФИШИНГ



Обход фильтров
вид фишинга, который использует изображение вместо текста, что затрудняет обнаружение мошеннических электронных писем антифишинговыми фильтрами

Социальная инженерия
вид фишинга, который своими действиями заставляет встревожить пользователя и вызвать у него немедленную реакцию

Неправомерная деятельность, направленная на преступное присвоение доступа к конфиденциальным данным пользователей, таким, как логины, пароли, данные пластиковых банковских карт и др.

Смишинг (SMS фишинг)
вид фишинга, который направлен на рассылку сообщений, содержащих ссылку на фишинговый сайт

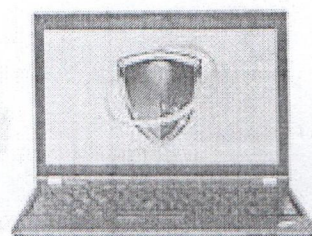
Веб-ссылки
вид фишинга, который призван замаскировать подделанные ссылки на фишинговые сайты под ссылки настоящих организаций

Веб-сайты
вид фишинга, который использует JavaScript для изменения адресной строки

Вишинг (голосовой фишинг)
вид фишинга, который направлен на создание сообщений на сайтах для пользователей о необходимости позвонить по определенному номеру для решения проблем с их банковскими счетами

Как уберечь себя от фишинга?

- Никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/CVV2 код).
- Пользуйтесь только защищенными сайтами: https (где «s» означает «secure» - безопасное).
- Не вносите какие-либо предоплаты за товар.
- Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети.
- Переходя на сайт банка проверяйте наличие защищенного входа (зеленая полоса перед строкой ссылки) и внимательно проверяйте внешний облик сайта.
- Не переходите по неизвестным ссылкам и не открывайте подозрительные электронные письма.
- Проверяйте адрес сайта, обращайте внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во всплывающей подсказке).
- Игнорируйте звонки и смс с неизвестных номеров и не заполняйте никакие формы в Интернете.



Всю информацию, поступившую посредством сети, обязательно проверяйте.

УМВД России по Сахалинской области

ВНИМАНИЕ!
ФИШИНГОВЫЕ АТАКИ

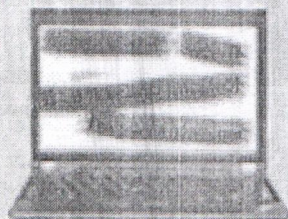
ОСТОРОЖНО МОШЕННИКИ!

ФИШИНГ – новый вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другое. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например от имени банков, сервисов или внутри социальных сетей. В эти письма мошенники вставляют ссылки на фальшивые сайты, являющиеся точной копией настоящих.



Чем опасны сайты-подделки?

- крадут пароли
- распространяют вредоносные ПО
- навязывают платные услуги



Как уберечь себя от мошенников?

- Никому не сообщайте свои персональные данные банковской карты (ПИН-код, CVC/CVV2 код, номер карты и дату окончания срока действия).
- Пользуйтесь только защищенными сайтами: https (где «s» означает «secure» - безопасное).
- Не вносите какие-либо предоплаты за товар, чтобы для вас его зарезервировали и не продали другому лицу, за возможное трудоустройство, а также в качестве аванса за сдачу жилья в наем.
- Оплачивайте товар по возможности при личной встрече и после проверки.
- Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети.
- Переходя на сайт банка проверяйте наличие защищенного входа (зеленая полоса перед строкой ссылки).
- Внимательно проверяйте внешний облик сайта.
- Не переходите по неизвестным ссылкам и не открывайте подозрительные электронные письма.
- Проверяйте адрес сайта, обращайте внимание на настоящий адрес сайта (при наведении мыши на реальный адрес отображается во всплывающей подсказке).
- Игнорируйте звонки и смс с неизвестных номеров и не заполняйте никакие формы в Интернете.



ПОМНИТЕ ВЫ МОЖЕТЕ СНИЗИТЬ УГРОЗУ ФИШИНГА, НЕМНОГО ИЗМЕНИВ СВОЕ ПОВЕДЕНИЕ

СТОП!!! МОШЕННИКИ!!!

ГДЕ ОБМАН?

ЧТО ДЕЛАТЬ?



ТЕЛЕФОН

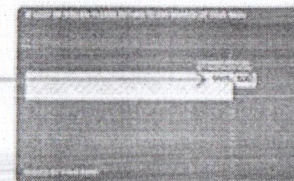
Вам звонят и, представившись сотрудниками банка, сообщают, что с Вашей карты совершается попытка перевода денег, снятия в банкомате, оформления кредита, оплаты товара, который Вы не заказывали

ПРЕРВИТЕ РАЗГОВОР,
НАБЕРИТЕ НОМЕР ВАШЕГО БАНКА

ПОЗВОНИТЕ В БАНК

Вам звонят под видом близкого родственника, попавшего в беду, или, представляясь сотрудником полиции, просят денег для решения проблемы

ПРЕРВИТЕ РАЗГОВОР,
ПОЗВОНИТЕ ВАШЕМУ РОДСТВЕННИКУ



ИНТЕРНЕТ

Вы покупаете товар на интернет-площадке (сайте)

ОПЛАЧИВАЙТЕ ТОЛЬКО ПРИ
ПОЛУЧЕНИИ ЗАКАЗА,
ПРЕДВАРИТЕЛЬНАЯ ОПЛАТА – ТОЛЬКО
НА ПРОВЕРЕННЫХ САЙТАХ

Вы продаете товар на интернет-сайтах

НЕ СООБЩАЙТЕ ПОКУПАТЕЛЯМ
СЕКРЕТНЫЙ КОД БАНКОВСКОЙ КАРТЫ
И НОМЕРА ПРИХОДЯЩИХ
СМС-СООБЩЕНИЙ

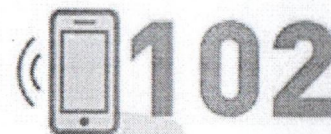


ДОМ

К вам в квартиру хотят попасть под видом сотрудников коммунальных служб, врачей, социальных работников или под предлогом продажи товара

НЕ ОТКРЫВАЙТЕ ДВЕРЬ

НАБЕРИТЕ НОМЕР БЛИЗКОГО
ЧЕЛОВЕКА. СООБЩИТЕ В ПОЛИЦИЮ



СТОП!!! МОШЕННИКИ!!!

ГДЕ ОБМАН?

ЧТО ДЕЛАТЬ?



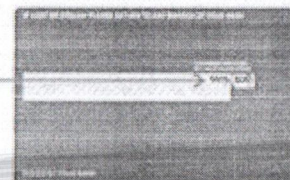
ТЕЛЕФОН

Вам звонят и, представившись сотрудниками банка, сообщают, что с Вашей карты совершается попытка перевода денег, снятия в банкомате, оформления кредита, оплаты товара, который Вы не заказывали

ПРЕРВИТЕ РАЗГОВОР,
НАБЕРИТЕ НОМЕР ВАШЕГО БАНКА

ПОЗВОНИТЕ В БАНК

НИКОМУ НЕ СООБЩАЙТЕ
СЕКРЕТНЫЙ КОД



Вам звонят под видом близкого родственника, попавшего в беду, или, представляясь сотрудником полиции, просят денег для решения проблемы

ПРЕРВИТЕ РАЗГОВОР,
ПОЗВОНИТЕ ВАШЕМУ РОДСТВЕННИКУ



ИНТЕРНЕТ

Вы покупаете товар на интернет-площадке (сайте)

ОПЛАЧИВАЙТЕ ТОЛЬКО ПРИ
ПОЛУЧЕНИИ ЗАКАЗА,
ПРЕДВАРИТЕЛЬНАЯ ОПЛАТА – ТОЛЬКО
НА ПРОВЕРЕННЫХ САЙТАХ

Вы продаете товар на интернет-сайтах

НЕ СООБЩАЙТЕ ПОКУПАТЕЛЯМ
СЕКРЕТНЫЙ КОД БАНКОВСКОЙ КАРТЫ
И НОМЕРА ПРИХОДЯЩИХ
СМС-СООБЩЕНИЙ

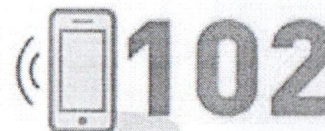


ДОМ

К вам в квартиру хотят попасть под видом сотрудников коммунальных служб, врачей, социальных работников или под предлогом продажи товара

НЕ ОТКРЫВАЙТЕ ДВЕРЬ

НАБЕРИТЕ НОМЕР БЛИЗКОГО
ЧЕЛОВЕКА. СООБЩИТЕ В ПОЛИЦИЮ



СТОП!!! МОШЕННИКИ!!!

ГДЕ ОБМАН?

ЧТО ДЕЛАТЬ?



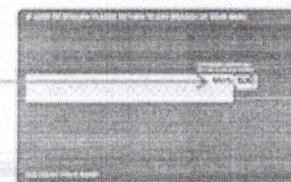
ТЕЛЕФОН

Вам звонят и, представившись сотрудниками банка, сообщают, что с Вашей карты совершается попытка перевода денег, снятия в банкомате, оформления кредита, оплаты товара, который Вы не заказывали

ПРЕРВИТЕ РАЗГОВОР,
НАБЕРИТЕ НОМЕР ВАШЕГО БАНКА

ПОЗВОНИТЕ В БАНК

НИКОМУ НЕ СООБЩАЙТЕ
СЕКРЕТНЫЙ КОД



Вам звонят под видом близкого родственника, попавшего в беду, или, представляясь сотрудником полиции, просят денег для решения проблемы

ПРЕРВИТЕ РАЗГОВОР,
ПОЗВОНИТЕ ВАШЕМУ РОДСТВЕННИКУ



ИНТЕРНЕТ

Вы покупаете товар на интернет-площадке (сайте)

ОПЛАЧИВАЙТЕ ТОЛЬКО ПРИ
ПОЛУЧЕНИИ ЗАКАЗА,
ПРЕДВАРИТЕЛЬНАЯ ОПЛАТА – ТОЛЬКО
НА ПРОВЕРЕННЫХ САЙТАХ

Вы продаете товар на интернет-сайтах

НЕ СООБЩАЙТЕ ПОКУПАТЕЛЯМ
СЕКРЕТНЫЙ КОД БАНКОВСКОЙ КАРТЫ
И НОМЕРА ПРИХОДЯЩИХ
СМС-СООБЩЕНИЙ

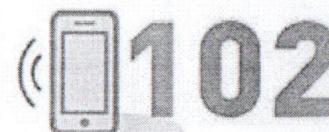


ДОМ

К вам в квартиру хотят попасть под видом сотрудников коммунальных служб, врачей, социальных работников или под предлогом продажи товара

НЕ ОТКРЫВАЙТЕ ДВЕРЬ

НАБЕРИТЕ НОМЕР БЛИЗКОГО
ЧЕЛОВЕКА. СООБЩИТЕ В ПОЛИЦИЮ



СТОП!!! МОШЕННИКИ!!!

ГДЕ ОБМАН?

ЧТО ДЕЛАТЬ?



ТЕЛЕФОН

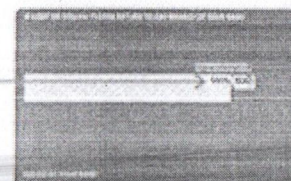
Вам звонят и, представившись сотрудниками банка, сообщают, что с Вашей карты совершается попытка перевода денег, снятия в банкомате, оформления кредита, оплаты товара, который Вы не заказывали

ПРЕРВИТЕ РАЗГОВОР,
НАБЕРИТЕ НОМЕР ВАШЕГО БАНКА

ПОЗВОНИТЕ В БАНК

Вам звонят под видом близкого родственника, попавшего в беду, или, представляясь сотрудником полиции, просят денег для решения проблемы

ПРЕРВИТЕ РАЗГОВОР,
ПОЗВОНИТЕ ВАШЕМУ РОДСТВЕННИКУ



ИНТЕРНЕТ

Вы покупаете товар на интернет-площадке (сайте)

ОПЛАЧИВАЙТЕ ТОЛЬКО ПРИ
ПОЛУЧЕНИИ ЗАКАЗА,
ПРЕДВАРИТЕЛЬНАЯ ОПЛАТА – ТОЛЬКО
НА ПРОВЕРЕННЫХ САЙТАХ

Вы продаете товар на интернет-сайтах

НЕ СООБЩАЙТЕ ПОКУПАТЕЛЯМ
СЕКРЕТНЫЙ КОД БАНКОВСКОЙ КАРТЫ
И НОМЕРА ПРИХОДЯЩИХ
СМС-СООБЩЕНИЙ



ДОМ

К вам в квартиру хотят попасть под видом сотрудников коммунальных служб, врачей, социальных работников или под предлогом продажи товара

НЕ ОТКРЫВАЙТЕ ДВЕРЬ

НАБЕРИТЕ НОМЕР БЛИЗКОГО
ЧЕЛОВЕКА. СООБЩИТЕ В ПОЛИЦИЮ



102

СТОП!!! МОШЕННИКИ!!!

ГДЕ ОБМАН?

ЧТО ДЕЛАТЬ?



ТЕЛЕФОН

Вам звонят и, представившись сотрудниками банка, сообщают, что с Вашей карты совершается попытка перевода денег, снятия в банкомате, оформления кредита, оплаты товара, который Вы не заказывали

ПРЕРВИТЕ РАЗГОВОР,
НАБЕРИТЕ НОМЕР ВАШЕГО БАНКА

ПОЗВОНИТЕ В БАНК

Вам звонят под видом близкого родственника, попавшего в беду, или, представляясь сотрудником полиции, просят денег для решения проблемы

ПРЕРВИТЕ РАЗГОВОР,
ПОЗВОНИТЕ ВАШЕМУ РОДСТВЕННИКУ



ИНТЕРНЕТ

Вы покупаете товар на интернет-площадке (сайте)

ОПЛАЧИВАЙТЕ ТОЛЬКО ПРИ
ПОЛУЧЕНИИ ЗАКАЗА,
ПРЕДВАРИТЕЛЬНАЯ ОПЛАТА – ТОЛЬКО
НА ПРОВЕРЕННЫХ САЙТАХ

Вы продаете товар на интернет-сайтах

НЕ СООБЩАЙТЕ ПОКУПАТЕЛЯМ
СЕКРЕТНЫЙ КОД БАНКОВСКОЙ КАРТЫ
И НОМЕРА ПРИХОДЯЩИХ
СМС-СООБЩЕНИЙ

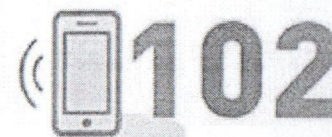


ДОМ

К вам в квартиру хотят попасть под видом сотрудников коммунальных служб, врачей, социальных работников или под предлогом продажи товара

НЕ ОТКРЫВАЙТЕ ДВЕРЬ

НАБЕРИТЕ НОМЕР БЛИЗКОГО
ЧЕЛОВЕКА. СООБЩИТЕ В ПОЛИЦИЮ



ВНИМАНИЕ МОШЕННИКИ!

с использованием ИНТЕРНЕТ

Продажа товара с использованием торговых интернет-площадок, интернет сайты «двойники» различных банков

ЗАПОМНИТЕ:

НЕ производите ПРЕДоплату какого-либо товара.

Деньги отдавайте только в том случае, если заказанный Вами товар проверен и полностью устраивает.

При входе на сайты известных Вам банков, организаций или торговых площадок внимательно изучайте открывшуюся страницу на экране.

с банковскими и кредитными картами

Вам поступило СМС-сообщение или звонок от лже-сотрудника банка о блокировке Вашей банковской карты и сообщения Ваших личных данных и данных Вашей карты или набрать комбинацию цифр в банкомате.

ЗАПОМНИТЕ:

НЕЛЬЗЯ перезванивать на предлагаемые Вам номера.

Сразу же связаться со службой поддержки банка, выпустившего Вашу кредитную карту, по телефонам, указанным на обратной стороне карты или лично посетить офис банка.

НЕЛЬЗЯ сообщать ПИН – КОД и КОД безопасности (напечатан на обороте).

НЕЛЬЗЯ набирать какие-либо комбинации цифр в банкомате, которые Вам диктуются по телефону якобы сотрудником банка (такая практика в банках отсутствует).

Будьте бдительны, не попадайтесь на уловки мошенников!

ВНИМАНИЕ МОШЕННИКИ!

с использованием ИНТЕРНЕТ

Продажа товара с использованием торговых интернет-площадок, интернет сайты «двойники» различных банков

ЗАПОМНИТЕ:

НЕ производите **ПРЕД**оплату какого-либо товара.

Деньги отдавайте только в том случае, если заказанный Вами товар проверен и полностью устраивает.

При входе на сайты известных Вам банков, организаций или торговых площадок внимательно изучайте открывшуюся страницу на экране.

с банковскими и кредитными картами

Вам поступило СМС-сообщение или звонок от лже-сотрудника банка о блокировке Вашей банковской карты и сообщения Ваших личных данных и данных Вашей карты или набрать комбинацию цифр в банкомате.

ЗАПОМНИТЕ:

НЕЛЬЗЯ перезванивать на предлагаемые Вам номера.

Сразу же связаться со службой поддержки банка, выпустившего Вашу кредитную карту, по телефонам, указанным на обратной стороне карты или лично посетить офис банка.

НЕЛЬЗЯ сообщать ПИН – КОД и КОД безопасности (напечатан на обороте).

НЕЛЬЗЯ набирать какие-либо комбинации цифр в банкомате, которые Вам диктуются по телефону якобы сотрудником банка (такая практика в банках отсутствует).

Будьте бдительны, не попадайтесь на уловки мошенников!

ВНИМАНИЕ МОШЕННИКИ!

с использованием ИНТЕРНЕТ

Продажа товара с использованием торговых интернет-площадок, интернет сайты «двойники» различных банков

ЗАПОМНИТЕ:

НЕ производите **ПРЕДоплату** какого-либо товара.

Деньги отдавайте **только** в том случае, **если** заказанный Вами **товар** проверен и **полностью устраивает**.

При входе на **сайты** известных Вам банков, организаций или торговых площадок **внимательно изучайте открывшуюся страницу** на экране.

с банковскими и кредитными картами

Вам поступило СМС-сообщение или звонок от лже-сотрудника банка о блокировке Вашей банковской карты и сообщения Ваших личных данных и данных Вашей карты или набрать комбинацию цифр в банкомате.

ЗАПОМНИТЕ:

НЕЛЬЗЯ перезванивать на предлагаемые Вам номера.

Сразу же связаться со службой поддержки банка, выпустившего Вашу кредитную карту, по телефонам, указанным на обратной стороне карты или лично посетить офис банка.

НЕЛЬЗЯ сообщать ПИН – КОД и КОД безопасности (напечатан на обороте).

НЕЛЬЗЯ набирать какие-либо комбинации цифр в банкомате, которые Вам диктуются по телефону якобы сотрудником банка (такая практика в банках отсутствует).

Будьте бдительны, не попадайтесь на уловки мошенников!

ВНИМАНИЕ МОШЕННИКИ!

с использованием ИНТЕРНЕТ

Продажа товара с использованием торговых интернет-площадок, интернет сайты «двойники» различных банков

ЗАПОМНИТЕ:

НЕ производите **ПРЕДоплату** какого-либо товара.

Деньги отдавайте **только** в том случае, **если** заказанный Вами **товар** проверен и **полностью устраивает**.

При входе на **сайты** известных Вам банков, организаций или торговых площадок **внимательно изучайте открывшуюся страницу** на экране.

с банковскими и кредитными картами

Вам поступило СМС-сообщение или звонок от лже-сотрудника банка о блокировке Вашей банковской карты и сообщения Ваших личных данных и данных Вашей карты или набрать комбинацию цифр в банкомате.

ЗАПОМНИТЕ:

НЕЛЬЗЯ перезванивать на предлагаемые Вам номера.

Сразу же связаться со службой поддержки банка, выпустившего Вашу кредитную карту, по телефонам, указанным на обратной стороне карты или лично посетить офис банка.

НЕЛЬЗЯ сообщать ПИН – КОД и КОД безопасности (напечатан на обороте).

НЕЛЬЗЯ набирать какие-либо комбинации цифр в банкомате, которые Вам диктуются по телефону якобы сотрудником банка (такая практика в банках отсутствует).

Будьте бдительны, не попадайтесь на уловки мошенников!

ВНИМАНИЕ МОШЕННИКИ!

с использованием ИНТЕРНЕТ

Продажа товара с использованием торговых интернет-площадок, интернет сайты «двойники» различных банков

ЗАПОМНИТЕ:

НЕ производите **ПРЕДоплату** какого-либо товара.

Деньги отдавайте **только** в том случае, **если** заказанный Вами **товар** проверен и **полностью устраивает**.

При входе на **сайты** известных Вам банков, организаций или торговых площадок **внимательно изучайте открывшуюся страницу** на экране.

с банковскими и кредитными картами

Вам поступило СМС-сообщение или звонок от лже-сотрудника банка о блокировке Вашей банковской карты и сообщения Ваших личных данных и данных Вашей карты или набрать комбинацию цифр в банкомате.

ЗАПОМНИТЕ:

НЕЛЬЗЯ **перезванивать на предлагаемые Вам номера.**

Сразу же **связаться** со службой поддержки банка, выпустившего Вашу кредитную карту, **по телефонам, указанным на обратной стороне карты** или **лично посетить офис банка.**

НЕЛЬЗЯ сообщать ПИН – КОД и КОД безопасности (напечатан на обороте).

НЕЛЬЗЯ **набирать какие-либо комбинации цифр в банкомате,** которые Вам диктуются по телефону якобы сотрудником банка (такая практика в банках отсутствует).

Будьте бдительны, не попадайтесь на уловки мошенников!