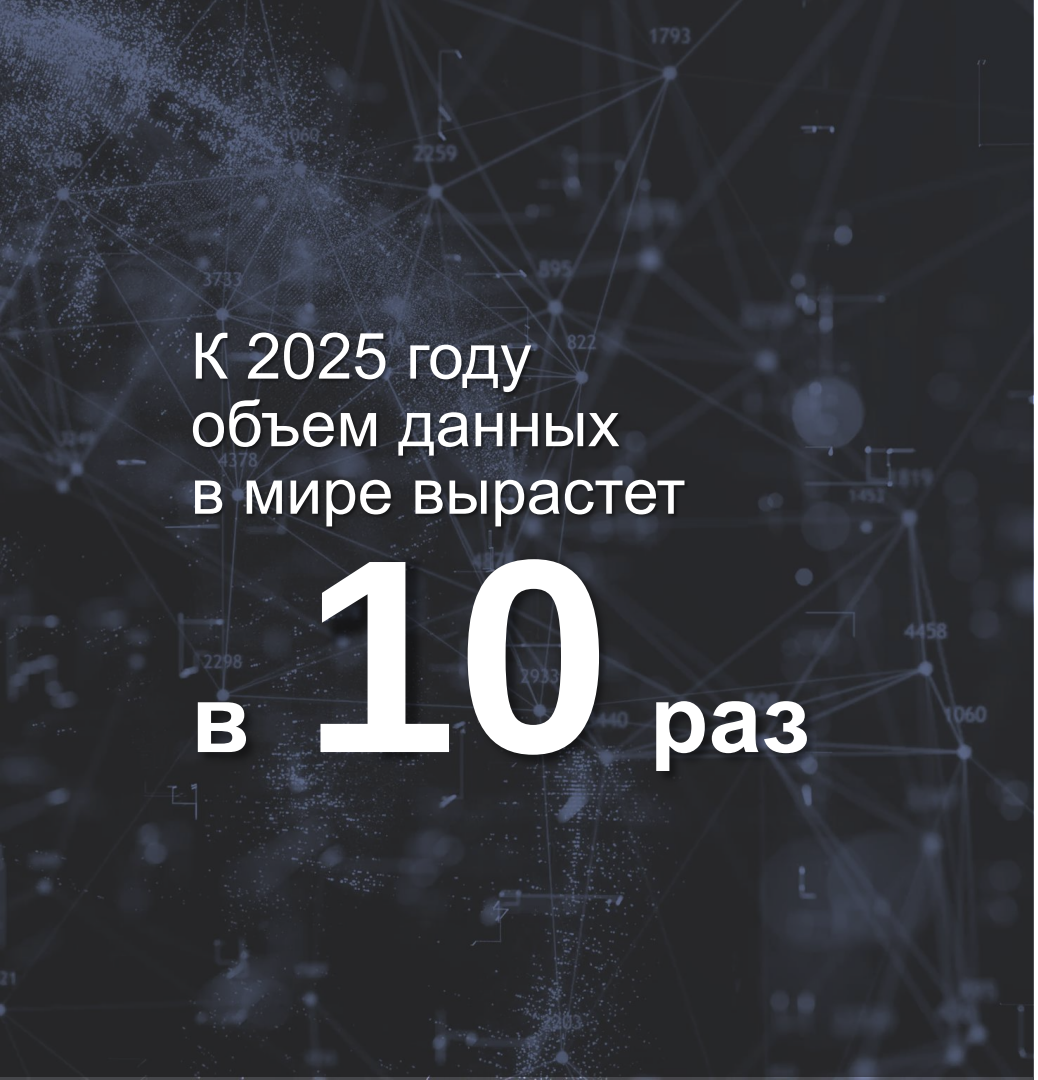
Принципы цифровой безопасности

Елена Бочерова

Исполнительный директор

КИБЕРПРОТЕКТ



Каждую минуту в мире

4 000 000
видео смотрят на YouTube

3 800 000
запросов «гуглят»
в поисковых системах

45 000
фото постят в соцсетях

Но не все данные одинаково полезны.

Цифровая среда полна не только возможностей, но и угроз

Информационная гигиена становится такой же привычкой как чистка зубов и мытье рук

10 правил цифровой безопасности

Мы выделили пять групп правил

- Входящий поток: скачиваем / открываем
- Исходящий поток: пишем, отправляем
- Платежи и покупки в интернете и в приложениях
- Пароли: как составлять и хранить безопасно
- Бэкап: зачем и как создавать резервные копии

КИБЕРПРОТЕКТ

Не скачивайте файлы и не вводите данные на подозрительных сайтах

Купили товар по подозрительной ссылке, что дальше?

Данные банковских карт попали к злоумышленникам и они получили доступ к вашим деньгам.

На ноутбук попали вирусы, они могут уничтожить или украсть ваши файлы. Мошенники будут шантажировать вас.

Встречаются сайты-двойники, проверяйте их подлинность

Как отличить небезопасные сайты и ссылки?

1. Длинное доменное имя, например, http://sberbank.master.supertalk.ru/lofiversion/index6326548.html
2. Предупреждение штатного антивируса
3. Навязчивая реклама и всплывающие окна
4. Не защищен сертификатом SSL: начинается с http://, а не с https://
5. Похож на официальный сайт, но URL-адрес изменен: не online.sberbank.ru, а onllinesberbank.ru

Что еще должно вас насторожить?

- ссылка в виде цифр http://178.248.232.27
- ссылка содержит символ @ http://bank.ru@zlo.ru
- ссылка содержит несколько адресов https://bank.ru/rd.php?go=https://zlo.ru
- в начале адреса сайта есть www, но нет точки или стоит тире wwwbank.ru или www-bank.ru
- буквы в ссылке заменены на цифры («о» на 0), прописная латинская буква заменена заглавной, произведена замена схожих по написанию букв (b на d) 0nline.dank.ru вместо online.bank.ru
- в начале адреса сайта есть http или https, но нет :// httpsbank.ru или httpbank.ru
- при наведении указателя мыши ссылка выглядит по-другому в тексте письма написано tele2.ru, а при наведении курсора teie2.ru

Не открывайте подозрительные электронные письма

Открывать письма с неизвестных адресов — как есть еду, которую нашел на улице: можно заразиться

Вам приходит письмо от неизвестной компании с выгодным предложением. К письму прикреплен файл, который на самом деле не является документом.

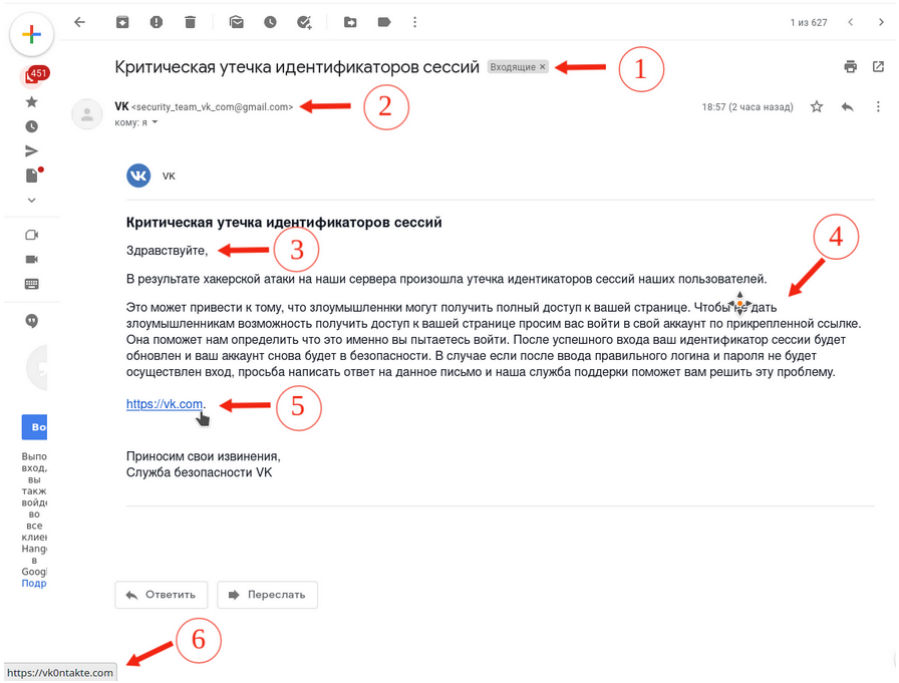
Если вы откроете файл, то активируете троянскую программу. Данные на вашем устройстве будут под угрозой.

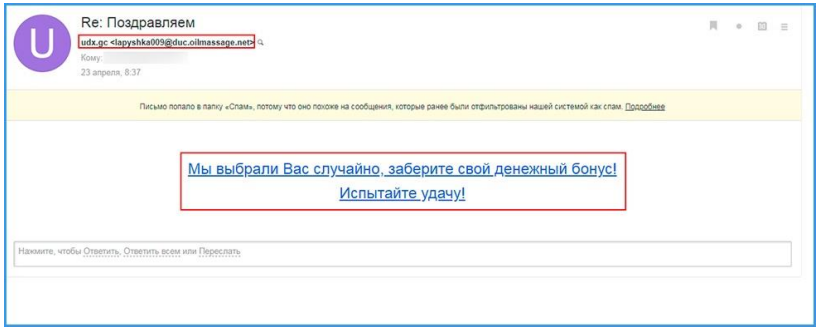
Как отличить подозрительное письмо?

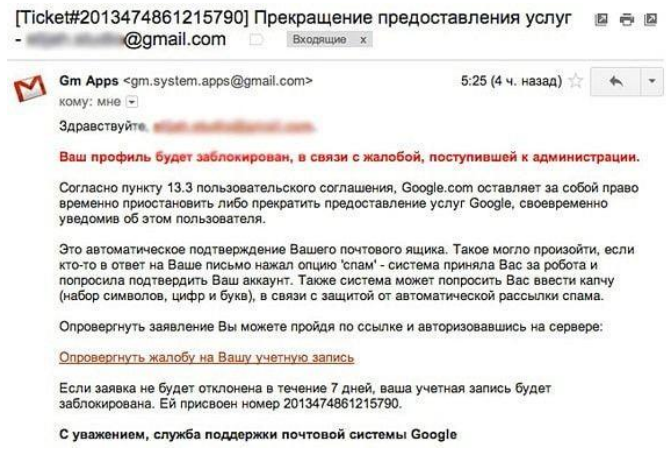
1. Неизвестный отправитель
2. Содержит срочную просьбу
3. Запрашивает личные данные или банковские реквизиты
4. Предложение слишком хорошо, чтобы быть правдой
5. «Кричащая» тема:
   «Заберите свой денежный бонус!»
6. В письме есть вложения, файлы:
   маленький размер файла, архив zip и rar
7. Содержит подозрительную ссылку

Банки и крупные организации не спрашивают личные данные по e-mail, проверьте почту, телефон, адрес отправителя на официальном сайте

Примеры фишинговых писем







Спам и приглашения в игры: часто это не игры, а ссылки на вредоносные программы!

Приглашения в игры, перепосты фотографий и постов про породистых щенков, которых нужно срочно спасать.

Розыгрыши телефонов и объявления «новый айфон в подарок всем, кто...» друзья могут расценить как спам.

Не добавляйте в друзья незнакомцев

Не доверяйте незнакомцам в Сети, они могут быть не теми, кем представляются. Как отличить фейковый аккаунт?

1. Страница создана недавно
2. Мало друзей, но очень много подписчиков
3. Фото залиты одним числом
4. Мало реальных фотографий
5. Нет постов от своего имени, только чужие репосты
6. Нет видео- и аудиозаписей

Как отличить мошенников?

Обещают легкие деньги:
«Вы выиграли в лотерею», «Заработать легко и быстро»

Запугивают:
«Ваша страница будет удалена через полчаса»

Давят на жалость:
«На корм бедным собачкам», «На дорогостоящее лечение»

Присылают рекламные сообщения, спам, ссылки на странные сайты

Просят проголосовать в опросах и конкурсах

Мошенники – талантливые манипуляторы. Если такие вещи присылает знакомый человек, но у вас есть подозрение, что его взломали – спросите то, что может знать только этот человек. Как правило, вам больше не ответят.

Меньше рассказывайте о себе в интернете!

Всё, что вы пишите в Интернете, остается там навсегда и может быть использовано против вас. Что не надо выкладывать в Сеть?

1. Точный адрес: фото с номерами домов, геолокации
2. Фото документов
3. Фото банковских карт
4. Билеты (на концерт, поезд)
5. Компрометирующие фото
6. Места учебы и проживания

Не всем приложениям нужен доступ к вашему местоположению, камере и интернету

К чему НЕ стоит давать доступ без необходимости:

1. Местоположение
2. Камера
3. Контакты и SMS
4. SD-карта
5. Управление временем «Сна»
6. Автозапуск системы
7. Контроль Wi-Fi соединения
8. Полный доступ к интернету

Ваше местоположение могут использовать мошенники. Доверяйте только известным и проверенным приложениям.

Агрессия в сети: мнимая виртуальность

Нам кажется, что в Сети можно писать агрессивно, оскорблять человека и за это ничего не будет!

Это иллюзия. Никогда не допускайте агрессии и оскорблений в интернете.

Грубые комментарии могут стать причиной упущенных возможностей в будущем. Компании-работодатели внимательно изучают виртуальную жизнь сотрудников.

Даже записи других людей могут использоваться против вас. Если друг выложит неловкое фото или видео с вами, вежливо попросите его удалить запись.

НЕ отправляйте деньги незнакомым людям

Суперприз, редкие болезни и помощь милым щенкам не повод переводить деньги незнакомцам.

Подумайте, что это за конкурс, существует ли такая болезнь.

Не сообщайте никому свои личные данные и данные карты, особенно информацию с обратной стороны.

Официальные компании никогда не используют для оплаты криптовалюту или биткойн

Шопинг в интернете

Заведите отдельную дебетовую карту и пополняйте ее на ту сумму, которую собираетесь оплатить

Не оплачивайте покупки, подключаясь к публичной сети WI-FI

Проверяйте ссылки, по которым проходит оплата

Создавайте надежные пароли и обеспечьте их безопасное хранение

Не менее 12 символов, включая буквы, цифры и символы

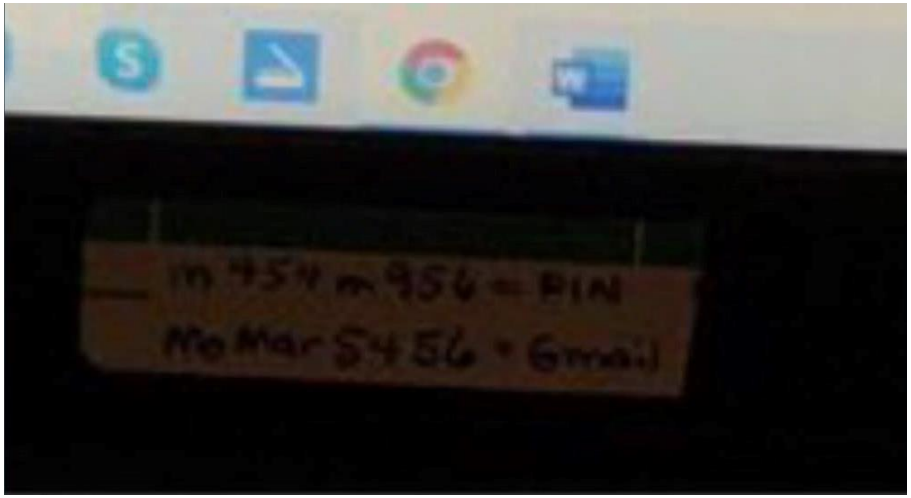
Не используйте для паролей личные данные: имя, город, дату рождения

По возможности используйте двухфакторную и многофакторную аутентификацию

1 ресурс = 1 пароль. Хранить их можно в менеджере паролей

Меняйте пароли, установленные по умолчанию

Храните пароли правильно и будьте внимательны!



Конгрессмен-республиканец от Алабамы и член комитета по кибербезопасности Пентагона Мо Брукс нечаянно опубликовал в Twitter пароль от Gmail и пин-код.

Хотел просто выложить снимок своего экрана, доказывая свою правоту в споре с оппонентом.

Создавайте резервные копии данных в облаке

Все цифровые данные могут быть уничтожены, поэтому применяйте Правило 3-2-1:

Иметь **три** копии данных

Хранить копии на **двух** разных носителях

Хранить **одну** резервную копию в облаке

КИБЕР
ПРОТЕКТ

Бесплатные курсы в рамках всероссийского проекта по обучению принципам безопасного поведения в сети Интернет:

- Курс повышения квалификации по цифровой гигиене для учителей средней школы
- Интерактивный курс для учеников 7-9 классов

Доступ к онлайн-курсам:
https://cyber-care.ru