

# ФИШИНГ ОТ РУКОВОДИТЕЛЯ

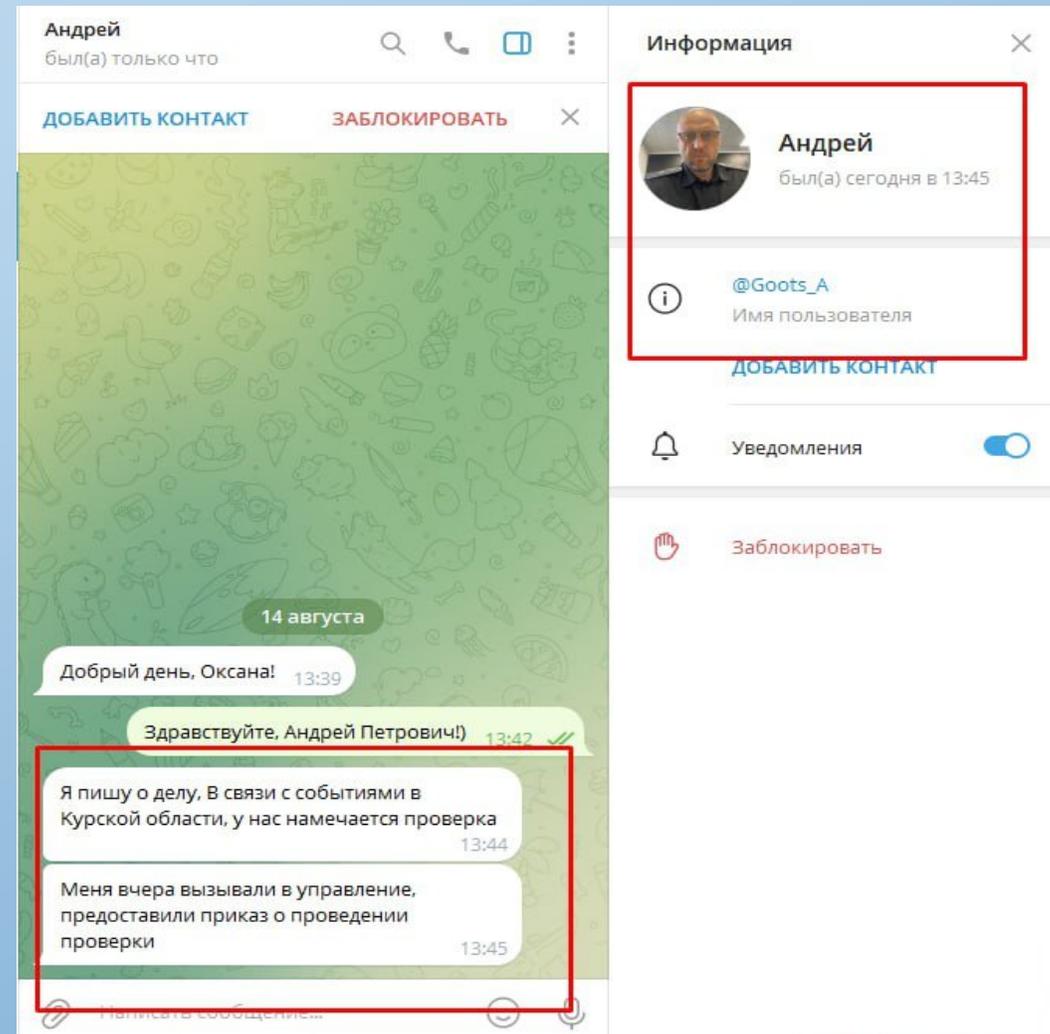
Министерство цифрового  
развития Белгородской  
области





# Пример фишинговых сообщений в мессенджере

Сообщения от лица якобы начальника Управления экологического и охотничьего надзора Белгородской области Гоца А.В.





# Пример фишинговых сообщений на электронной почте

Сообщения с украденной учетной записи начальника отдела взаимодействия с органами власти области и муниципальными образованиями министерства общественных отношений о якобы возникшей угрозе кибератаки

Срочное сообщение об угрозе кибератаки на государственные информационные ресурсы Белгородской области

 Зинченко Андрей Валерьевич  
Сегодня, 10:32  
ofks31@mail.ru; shebetenko2011@yandex.ru; ivlyanova@be.belregion.ru; detigv@mail.ru; taryanik\_dk@dizo31.ru; belozerskih@be.belregion.ru; и еще 94 получателей

Ответить всем

Пометка к исполнению. Начало: 12 марта 2024 г. Срок: 12 марта 2024 г.

 AV\_Scan.rar  
183 КБ

Скачать

В ночь с 11.03.2024 на 12.03.2024 государственные информационные ресурсы Белгородской области подверглись кибератаке. Вредоносное программное обеспечение шифрует данные на компьютерах без возможности их восстановления. Правительство Белгородской области информирует Вас о необходимости обязательного выполнения п.1.2.1 протокола решений заседания оперативного штаба Белгородской области от 12 марта 2024 года № 14, а также распоряжения начальника управления региональной безопасности Белгородской области Воробьева Е.В. от 12 марта 2024 года № 348-р. Вам необходимо выполнить следующие действия для предотвращения (устранения) последствий кибератаки:

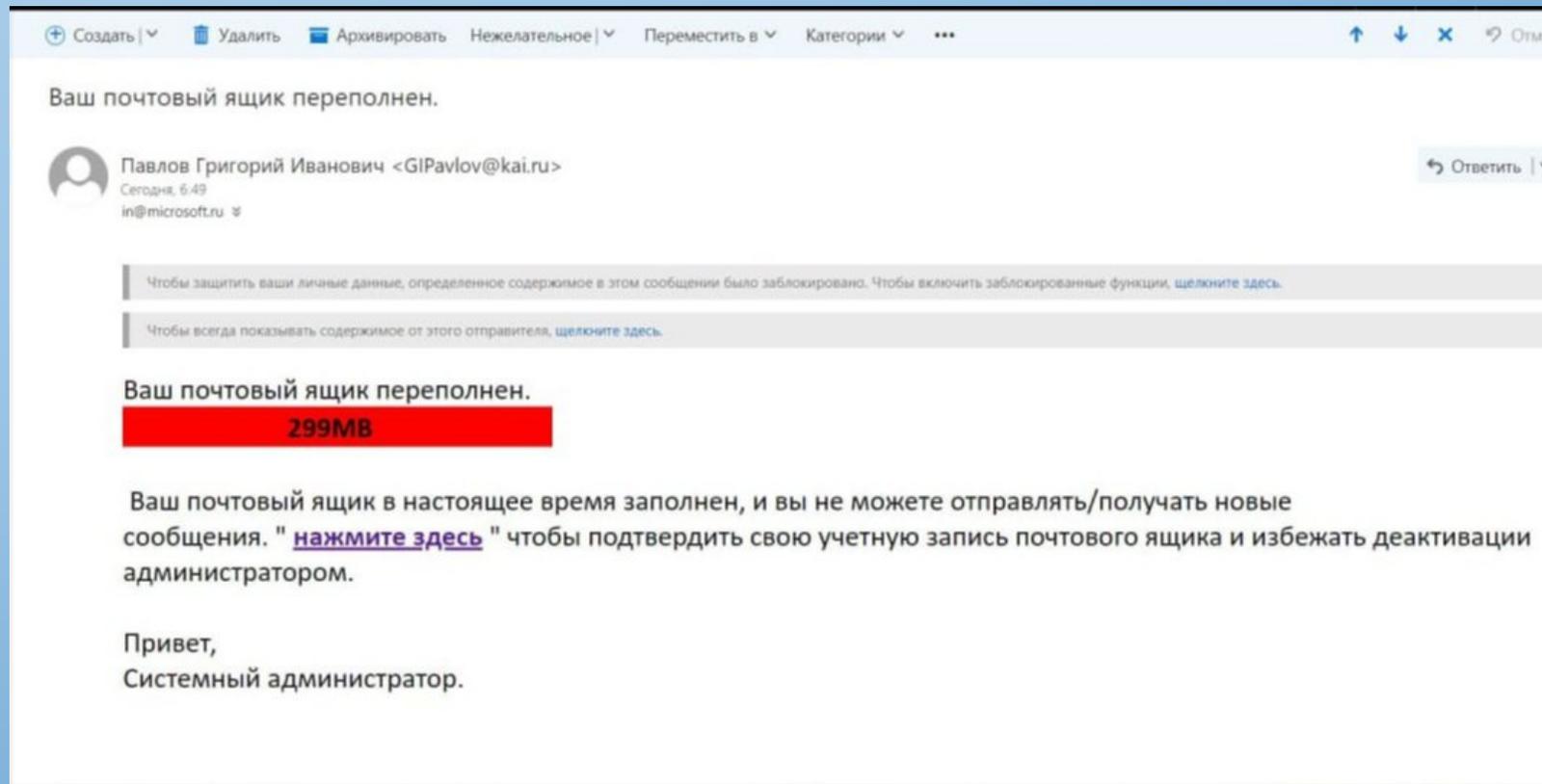
1. Загрузить архив во вложении к данному сообщению.
2. Распаковать архив (пароль: fnt38z ).
3. Запустить утилиту AV\_Scan.exe.
4. По завершению работы утилиты отправить отчет о выполнении на адрес электронной почты оперативного штаба (управления региональной безопасности) Белгородской области sssb\_pr@belregion.ru.

Зинченко А.В.,  
начальник отдела  
Министерство общественных коммуникаций Белгородской области

# Пример фишинговых сообщений на электронной почте

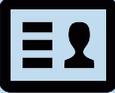


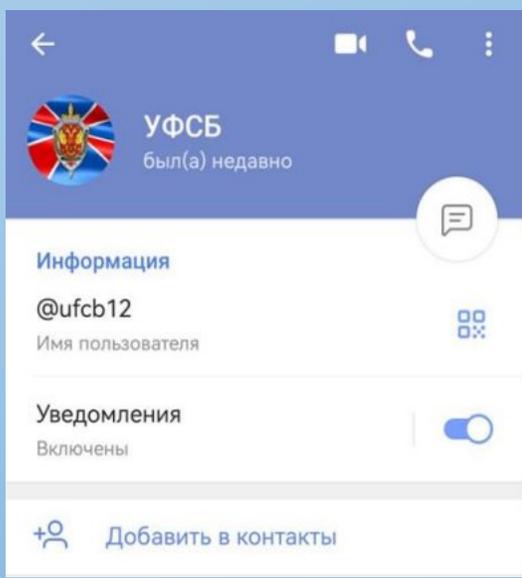
Сообщения о переполненном почтовом ящике от якобы системного администратора организации





# Уловки мошенников. Примеры

-  Подменяют номер телефона на официальный
-  Направляют фото якобы своего служебного удостоверения
-  Используют официальную символику органов государственных власти



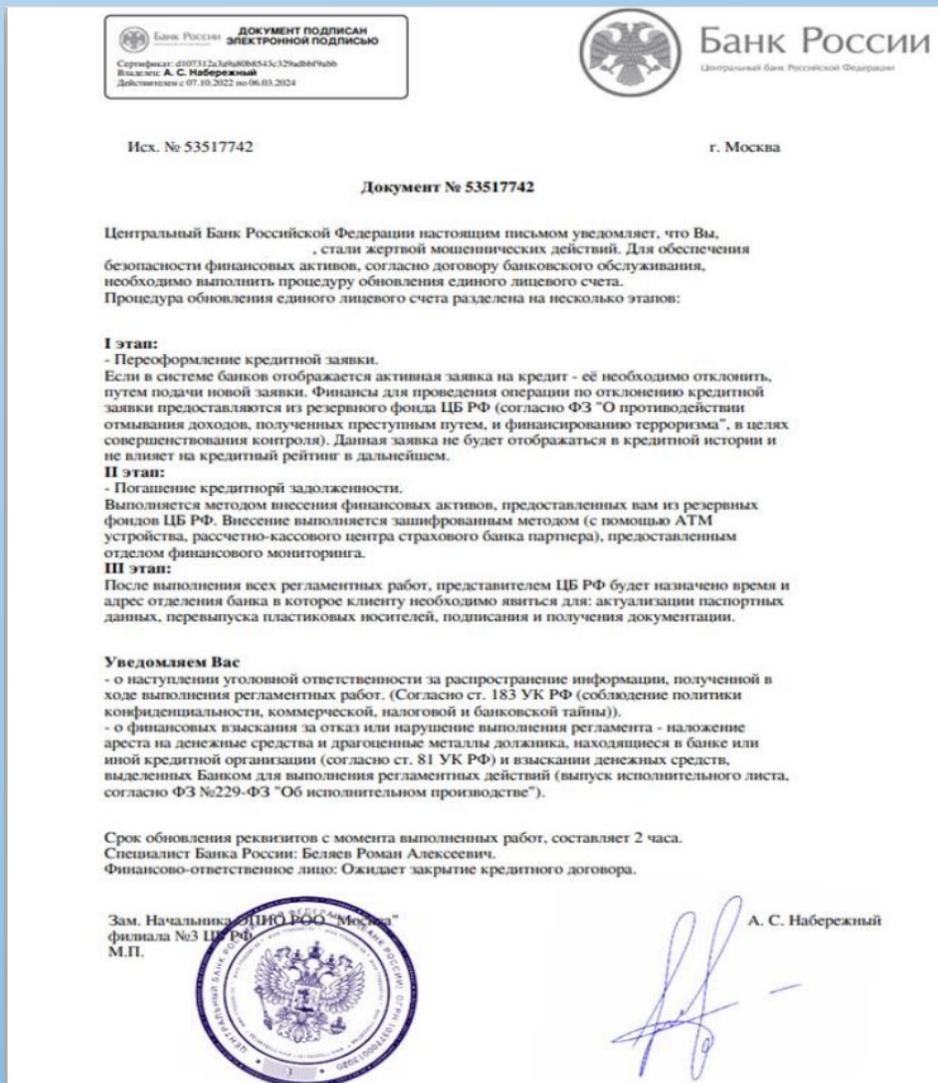
# Уловки мошенников. Примеры



Мошенники направляют от имени органа государственной власти (УФСБ России по Белгородской области) якобы официальное обращение, заверенное подписью и печатью руководителя, о проведении внеплановой проверки органа (организации) и привлечении к ответственности сотрудников



# Уловки мошенников. Примеры



Мошенники направляют от имени органа государственной власти (Банк России) якобы официальное обращение, заверенное подписью и печатью руководителя, о необходимости выполнения процедуры обновления единого лицевого счета





# Что делать, если вы получили письмо от лица руководителя вашей организации?

- ✓ Прекратите какое-либо общение с мошенником. Вас могут начать пугать фотографиями служебных удостоверений, официальных документов и тому подобным. Не поддавайтесь давлению!
- ✓ Расскажите своему непосредственному руководителю о факте обращения от лица руководителя Департамента или вашей организации
- ✓ Дождитесь от непосредственного руководителя подтверждения достоверности обращения от руководителя Департамента или организации
- ✓ В случае, если это всё-таки были мошенники, напишите об инциденте на почту: [ddd@belregion.ru](mailto:ddd@belregion.ru) и [avz@belregion.ru](mailto:avz@belregion.ru)
- ✓ В случаях, если вы подверглись манипуляции и совершили какие-либо действия со своим банковским счетом, немедленно обращайтесь в банк для блокирования переводов и в правоохранительные органы - с заявлением о мошенничестве





# «От имени руководителя» - теперь и голосом

Используя современные технологии, мошенники генерируют фейковые ГОЛОСОВЫЕ СООБЩЕНИЯ, которые отправляют через мессенджеры

## Будьте бдительны если:



сообщение выходит за рамки привычного обсуждения - например, связано с денежным переводом, запросом пароля, необходимостью взаимодействия с правоохранительными органами и т.п.



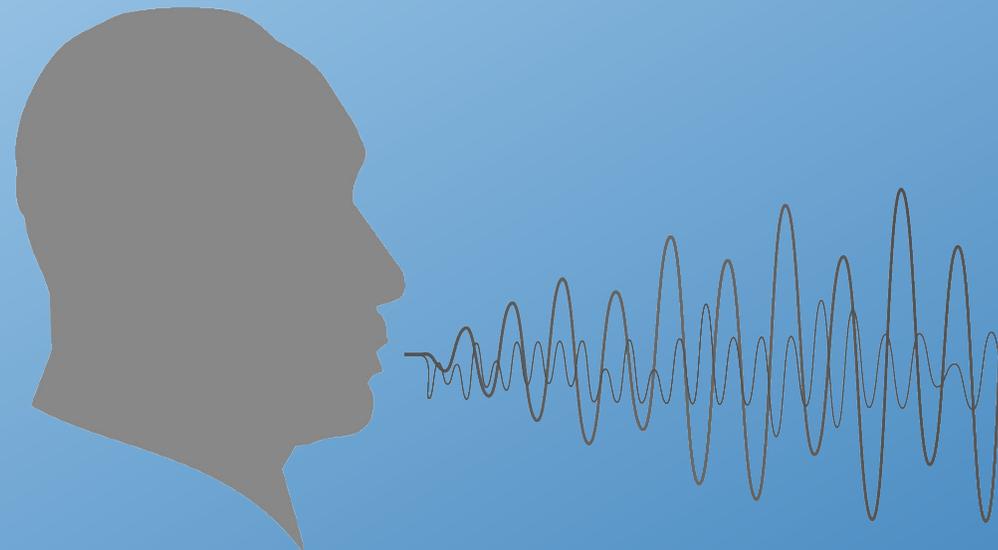
вы не ждали личного сообщения от руководителя



в сообщении присутствует давление через свой авторитет



в сообщении присутствует момент срочности



# ФСТЭК России рекомендует



## Письма ФСТЭК России

От 29.12.2023 № 240/22/6370

«...Хакерской группировкой Core Werewolf осуществляются компьютерные атаки на информационную инфраструктуру РФ, путем направления от имени ФСТЭК России «фишинговых» электронных писем с именем домена отправителя «cfo\_11otd@fstec.support.», содержащих вредоносный архив с наименованием «Меры. Список уязвимостей и принимаемых мер по их устранению.exe»...»

От 19.01.2024 № 240/91/208

«...Хакерской АPT-группировкой Sticky Werewolf в адрес ФОИВ, субъектов КИИ и организаций РФ направляются фишинговые письма от имени ФСБ России, МЧС России и Минстроя России, а также иных органов и организаций, содержащие вредоносные вложения (трояны Darktrack RAT, Ozone RAT, стилер MetaStealer)»...».

### Обращаем внимание!

- ✓ ФСТЭК России осуществляет взаимодействие посредством системы МЭДО, почтовой связи и электронной почты (домен @fstec.ru).
- ✓ При получении электронного письма от имени ФСТЭК России, необходимо связаться с ответственным исполнителем по ранее направленным ФСТЭК России письмам, перезвонив ему по телефону

# Всегда на связи!

Министерство  
цифрового развития  
Белгородской  
области



[ddd@belregion.ru](mailto:ddd@belregion.ru)

