Цифровая гигиена

- Не понимаю, как они смогли взломать у меня пароль на почту?
- А что у тебя за пароль был?
- Год канонизации святого Доминика папой Григорием IX
- А это какой год?
- 1234 …

Распределение усилий по общей безопасности

- Существуют ряд технических средств усложняющий получение логина/паролями и контроля за почтовыми ящиками пользователей. Этим занимаются системные администраторы НИВЦ.
- Здесь рассматривается только вторая часть технической коллаборации – собственно, действия и политика поведения пользователей почтового сервиса.

Принципы работы электронной почты

- Письмо создается на компьютере пользователя (в почтовом клиенте или через web-интерфейс)
- Пользователь идентифицируется логином и паролем на почтовом сервисе (при подключении с любого места) и передаёт почтовому сервису письмо для дальнейшей отправке получателю
- Почтовый сервер от имени Организации занимается конечной доставкой почты от «своих» пользователей респондентам
- Почтовый сервер считает легитимным письмо с любым содержанием от «своих» авторизовавшихся пользователей (отсутствует перлюстрация)

- При возникновении проблем с отдельным почтовым ящиком санкции накладываются на весь почтовый сервис, т.е. на **всех** пользователей …

Инцидент с «утечкой» пароля

- После того, как пароль одного из пользователей НИВЦ стал известен злоумышленникам, от его имени было отправлено 63902 письма, в каждом по несколько получателей.
- Нашим почтовым сервером было доставлено 350120 писем спама.
- Удалось предотвратить доставку еще 282111 писем.
- Расчистка почтовой очереди заняла 3 часа, в течении которых почтовый сервер НИВЦ не работал.
- Наш почтовый сервер попал в публичные спамовские фильтры как неблагонадёжный. Необходимо связываться с каждым таким сервисом и отчитываться о том, что проблема устранена.

Подбор пароля –> «сложный» пароль

- НЕ выбирать короткий пароль
- НЕ использовать обычные слова из словарей для пароля или его части
- Никому НЕ сообщать свой пароль
- НЕ вводить свой пароль на устройствах, к которым нет доверия (интернет-кафе)
- НЕ переходить по неизвестным ссылкам из почты и в браузере
- НЕ нажимать кнопку «ОК» без внимательного изучения текста предложения

- Длина пароля больше 8 символов
- Использовать начальные буквы (или слоги) из фраз
- Использовать в пароле заглавные и прописные буквы
- Использовать в пароле цифры
- Использовать в пароле символы: !#$^&*-_+

Примеры «*хороших*» сложных паролей

- Русские слова в английской раскладки клавиатуры:
  Академический_Институт -> Frfltvbxtcrbq_Bycnbnen
- Акроним – первые буквы какой-то (не очень распространённой) фразы
  “Наука может много гитик” – НмМг…
- Использовать слоги из какого-то предложения: “Research Computer Center of Moscow State University” -> RePuTer_Mo$t@Un…
- Прочесть получившийся пароль целиком – не напоминает ли он целиком или его часть реальное слово из словаря
- К сгенерированной части паролей добавлять символы (!#$^&*-_+) и цифры

- **Не использовать одинаковый пароль для всего – если его взломают (утечёт) – злоумышленники получат доступ ко ВСЕМ вашим ресурсам!**

Вычислительные ресурсы по подбору паролей

- Фирма по кибербезопасности Home Security Heroes опубликовала исследование, в котором показала работу инструмента на основе ИИ PassGAN для проверки более 15 680 000 паролей. Он смог подобрать 51% *распространённых* паролей менее чем за минуту. С помощью брутфорса было взломано 65% паролей менее чем за час, 71% был подобран менее чем за день и 81% — менее чем за месяц.
- Если используется 12-значный пароль, состоящий из прописных и строчных букв, инструменту может потребоваться 289 лет, чтобы взломать его. При добавлении цифр этот срок увеличивается до 2000 лет, а символов — до 30 000 лет.

• Все вышесказанное относится к любым компьютерным паролям – банковским аккаунтам, сервисам госуслуг и другим важным сервисам

Спасибо за сотрудничество

• Проверить сложность ваших паролей можно по ссылке: https://www.homesecurityheroes.com/ai-password-cracking/

для проверки вводите похожий, а не свой ***реальный*** пароль