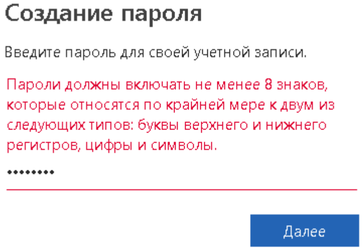
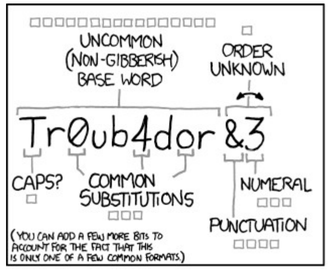
КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Инструктаж сотрудников по ИБ. Методика и практика

Виктор Буренков





SecurityLab.ru

Основные вопросы

Кого следует инструктировать?

Что включить в инструктаж?

Инструктаж и должностная инструкция: отличия

Обратная связь пользователей с подразделением ИБ

Предпосылки инструктажа по информ. безопасности

• Недостатки текстовых инструкций:
- «подписал и забыл» (воспринимается как формальность);
- важные пункты не поняты.

• Если есть подразделение ИБ:
- инструктаж — возможность консультации со специалистом;
- создаём обратную связь сотрудников с подразделением ИБ.

• Возможно проведение ИБ-инструктажа не только ИБ-специалистами

Кого инструктируем?

«Разработчиков, системных администраторов инструктировать по ИБ не нужно, поскольку они и так опытные компьютерщики».

Практика показывает, что множество утечек происходит по вине разработчиков и квалифицированного ИТ-персонала.

Пример: Яндекс, .svn-base

Варианты инструктажа

Первичный и регулярный

По очерёдности:
• плановый;
• внеплановый
(реагирование на инцидент).

По форме:
• рассылка письма;
• беседа или семинар.

Варианты изложения содержания
• пересказ (вспомните стюардесс);
• интерактивный.

Основа интерактивного инструктажа — вопросы пользователю.

Нужен доброволец!

Интерактивный инструктаж

Возможен на стадии приёма в штат.

Ставит целью действенно повысить бдительность сотрудника в эпоху спама, фишинга и шифровальщиков

Запоминается лучше, чем при росписи под текстом.

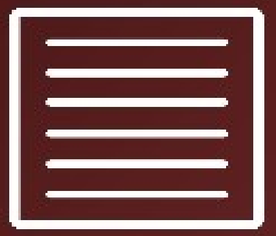
Можно проводить индивидуально или с небольшими группами.

Очень часто можно продемонстрировать подтверждение взломов бесплатной почты пользователя.

https://haveibeenpwned.com
и типовая выдача для засвеченного в утечках адреса

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Exploit.In (unverified): In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I been pwned.

Compromised data: Email addresses, Passwords

VK: In approximately 2012, the Russian social media site known as VK was hacked and almost 100 million accounts were exposed. The data emerged in June 2016 where it was being sold via a dark market website and included names, phone numbers email addresses and plain text passwords.

Compromised data: Email addresses, Names, Passwords, Phone numbers

Какие темы важно затронуть

1

USB-накопители
Можно объяснить, что они не актуальны по нескольким причинам, не только из соображений ИБ

2

Электронная почта
Один из главных векторов атаки на корпоративный сегмент

3

Бесплатные сервисы и социальные сети
Не используйте пароли оттуда в служебных учётных записях, и будет Вам счастье! И компании тоже.

4

Один пользователь — один пароль
Служебный пароль не вещь, которую передают в пользование. За действия под Вашим логином будут спрос с Вас

5

Фишинг, шифровальщик, социальная инженерия, …
Пусть для пользователя эти слова станут так же понятны, как «селфи», «мем», «трансляция» — пусть больше задумываются об угрозах

6

Держите контакт с ИБ
Всегда можно обратиться с вопросом в случае сомнений (подозрительное письмо и т. д.)

Ваши пункты

Информационная безопасность должна учитывать вид и специфику деятельности

1

2

3

4

5

6

Ещё один общий пункт

Небольшая оговорка: современная криптография подразумевает систему, в которой ключ является единственным секретом; алгоритмы шифрования открыты и, как правило, подлежат разглашению.

«Перспективные» утечек служебных данных (интернет)

1 **VK.com**

2 **Сервисы загрузки изображений**

3 **Файлообменники**

4 translate.yandex.ru
translate.google.com

5 **pastebin**

6 **TeamViewer**

Подробнее по теме «фишинг»

Задумайтесь, прежде чем переходить по ссылкам из письма.

Совпадает ли фактический адрес ссылки с отображаемым в письме?

Посмотрите внимательнее на адрес отправителя. Адрес Вам знаком?

Внушает ли Вам доверие текст письма? Если, например, в тексте слишком много орфографических ошибок для официального письма — скорее всего, письмо подделано.

Есть ли вложения в письме? Задумайтесь, Вы отправляли бы вложение в подобной ситуации? Если нет веских причин на наличие вложения — следует с отнестись с подозрением к вложению.

Подробнее по теме «пароли»

Задумайтесь, где Вы вводите служебный пароль, и надо ли там его вводить?

В зависимости от конфигурации систем можно проинструктировать, например, пароль вводим только при входе в компьютер и никогда не вводим в браузере

Подробнее: Ваши действия

Если случайно допустили действие, не исключающее риск — перешли по вредоносной ссылке, открыли вложение с Macros или просто увидели лишнее всплывающее окно — **обратитесь в подразделение информационной безопасности!**

Подразделение ИБ — ваш друг в борьбе с угрозами.

Если Вам пришло подозрительное письмо — перешлите его нам на адрес itsec@yourcompany.com — мы посмотрим!

Доверительное отношение к подазделению ИБ — залог успеха!

О паролях

Как правильно выстроить парольную политику и соответствующий инструктаж *в зависимости от условий*?

Конец XX века

- секретный вопрос
- кодовое слово
- пароль

Год 2019-й

- ok.ru

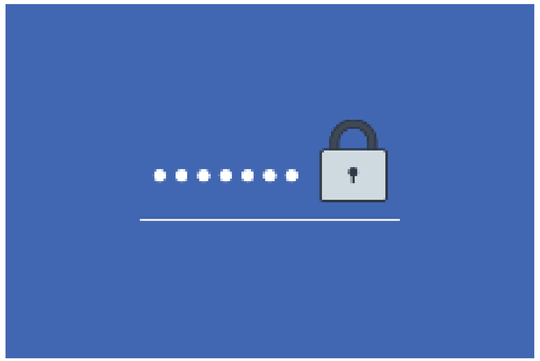
Нужна девичья фамилия матери?
Вам сюда!

- поразвлекаемся с кол-центром
- 20 лет спустя: что изменилось в мире паролей?

Шёл 2019-й год...

08:44 / 25 Апреля, 2019

Microsoft признала бесполезной политику устаревания пароля



Теги: Microsoft, Windows 10, пароль

Компания откажется от механизма устаревания паролей в обновлении Windows 10 May 2019 Update.

Компания Microsoft решила отказаться от политики устаревания паролей, которая требует от пользователей периодически менять установленные пароли. Техногигант представил новый проект плана базовых настроек конфигурации для Windows 10 v1903 (19H1) и Windows Server v1903, который устраняет необходимость каждые несколько недель или месяцев менять пароли в учетных записях, находящихся под управлением групповых политик. Нововведение будет реализовано в обновлении Windows 10 May 2019 Update, релиз которого ожидается в мае нынешнего года.

Как поясняется в блоге Microsoft, существующая политика «древняя и устаревшая мера, имеющая низкую ценность», и компания больше не верит «в ее целесообразность». Механизм устаревания паролей, который требует периодической смены пароля, сам по себе ненадежный метод защиты, учитывая, что при краже пароля следует оперативно принимать меры, а не ждать, пока закончится срок его действия, отмечают в компании.

The top 10 most common passwords were:

- 123456.
- 123456789.
- qwerty.
- password.
- 111111.
- 12345678.
- abc123.
- 1234567.

Ещё • 23 апр. 2019 г.

The most commonly hacked passwords, revealed - CNN - CNN.com

https://www.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr.../index.html

Если пользователи создают такие пароли, нужны ли они в принципе, когда есть второй фактор авторизации?

MasterPass: не нужны
YubiKey: (тем более) не нужны
...

В информационных системах компаний (AD), как правило, по-прежнему без альтернатив.

Реальность: пользователи создают пароли «Qwerty123», «Ivanova20» и подобные на грани удовлетворения парольной политики

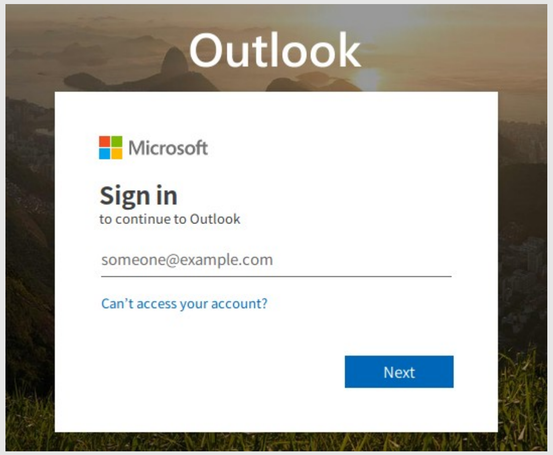
Когда «123456» и «qwerty» особенно опасны?

1

Удалённый доступ

VPN, RDP-шлюз, ...

2



Знакомая картинка?

Любой web mail, интегрированный с AD

Дополнительная трудность

Если пользователь удовлетворил требования парольной политики, то при правильной схеме хранения пароля нет этического способа дополнительной проверки качества заданного пароля.

Что делаем с «123456» и «qwerty»?

Если у пользователя не подключен удалённый доступ — в принципе, большой угрозы нет. Главное, чтобы коллеги не подобрали пароль.

Если **удалённый доступ** необходим — объясняем о необходимости установить **стойкий пароль** и предупреждаем об ответственности.

Контрмеры (отдельная тема).

Выводы

Проводите инструктаж по ИБ при приёме на работу и регулярно для действующих сотрудников. Посвящайте пользователей в современные явления и понятия в мире киберугроз и информ. безопасности.

Убедите пользователя в рисках на его собственном примере.

Нельзя использовать в служебных учётных записях пароли от бесплатных сервисов. Также следует ограничить регистрацию в сервисах на служебную почту.

Выводы

Повышайте бдительность пользователей в части фишинговых атак, в части подозрительных признаков при работе с программами.

Наладьте обратную связь. Пусть станет нормой обращение за консультациями к ИБ-специалистам.

Создайте специальный адрес для пересылки подозрительных писем на дополнительную проверку специалистами по ИБ.

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ!

victor.burenkov@yahoo.com

+7 962 3268935

Skype: vburro