ФИШИНГ

ПОНЯТИЕ О ФИШИНГЕ

Фи́шинг (от английского fishing — рыбная ловля, выуживание) это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам, паролям, данным кредитных карт, номерам телефонов, паспортным данным и другим чувствительным данным, а также запуск вредоносного программного обеспечения на компьютере пользователя.

Такой вид интернет-мошенничества, как правило, основан на психологической манипуляции и его **цель – вывести человека на** такие **эмоции**, как:

- **интерес**
- **страх**
- **жадность**
- **злость**
- **желание помочь**

Это позволяет ослабить концентрацию человека, **усыпить его бдительность.**

ЦЕЛЬ ФИШИНГОВА ПИСЬМА – ЗАСТАВИТЬ ПОЛУЧАТЕЛЯ:

Перейти на мошеннический сайт:

- после нажатия на фишинговую *ссылку* в письме или во вложенном файле
- после нажатия на фишинговую *кнопку* в письме

Заразить устройство (компьютер, планшет, смартфон) получателя:

- после открытия фишингового (зараженного) файла
- после перехода на зараженный сайт (при нажатии на вредоносную ссылку получатель письма перенаправляется на сайт, эксплуатирующий уязвимости браузера)

ПРИЗНАКИ ФИШИНГОВЫХ ПИСЕМ:

1. **Тема, контент письма, названия файлов побуждают получателя к спешке, к немедленному действию** (к переходу по ссылке, к нажатию на кнопку, к открытию файла, к немедленному ответу на письмо).

Здесь в полную меру **используются эмоции, чувства, страхи, рефлексы.**

Например:

- *«У Вас не погашен кредит», «Ваше сообщение не доставлено», «Ваша почта будет заблокирована» - используется страх,*
- *«Подравляем! Лотерейный Билет на Ваше имя оказался выигрышным! Заберите свой выигрыш: Ссылка» - используется любопытство и жадность*

2. **В подписи к письму обычно нет обратного телефона отправителя,** либо вообще не указан отправитель

3. **Обращение к получателю обычно обезличенное** (если это не целевой фишинг)

Например: «Здравствуйте», «Уважаемый клиент»

4. **В письме используется автоподстановка** для обращения к получателю

Например: «Уважаемый <имя почтового ящика (до символа @)>»

5. Часто письма отправляются **от имени известных компаний** (логистических компаний, банков, платежных систем, органов судебной или исполнительной власти, олимпийских комитетов), **известных людей** (*указание таких отправителей тоже воздействует на психологию получателей, так как вызывает рефлекторное доверие*)

ПРИЗНАКИ ФИШИНГОВЫХ ПИСЕМ:

6. **Отправители,** выдают себя за официальных представителей известных компаний (в том числе, выдают себя за Ваших коллег), но **пишут с общих почтовых доменов gmail.com, mail.ru и т.п.,** а не с корпоративных адресов

7. **Письмо требует ввести конфиденциальные данные**

8. **Письмо содержит какие-то документы, которые надо открыть**

   *Например, либо какие-то «счета» - «invoice.doc», «Penalty Receipt.docm», либо просто какие-то документы «New doc 115.docm», «unnamed document.docm», **якобы сканкопии**. Вложения могут быть в виде doc, docm, pdf-файлов, архивов arj, zip, rar, исполняемых exe-файлов и в других форматах*

9. **Письмо содержит ссылки,** в том числе, замаскированные под изображения, документы, QR-коды, **и другие активные объекты** (кнопки и т.п.), переводящие на другие сайты или загружающие файлы

10. **Текст ссылок в письме не совпадает с реальными ссылками**

11. Строка адреса сайта в ссылке содержит спецсимвол «@» или другие странные символы

    Например, такой адрес http://google.com@fishing.com/anything означает, что ссылка Вас направит на сайт fishing.com, а не на google.com

ПРИМЕР ФИШИНГОВОГО ПИСЬМА:

Для злоумышленника **не составляет труда найти** в открытых источниках **информацию о структуре организации, определить ключевых должностных лиц** и домен корпоративной почты организации. Это позволяет злоумышленнику сделать фишинговую рассылку примерно следующего содержания:

«Уважаемый ….!

В период с 1 марта по 3 апреля будет производится ревизия почтовых ящиков …. Все неиспользуемые почты будут отключены. Если вы получили данное письмо и планируете использовать данный почтовый ящик в будущем, просьба оперативно войти в личный кабинет по следующей ссылке:……..»

Ссылка, конечно же, ведет на **поддельную** форму авторизации. Если сотрудник вовремя не поймет, что данная рассылка является фишинговой, и перейдет по ссылке, он окажется на странице, которая внешне неотличима от настоящей формы ввода учетных данных. Конечно же, введя логин и пароль, такой сотрудник **«добровольно»** предоставит доступ к своим данным злоумышленникам.

ПЕРВОНАЧАЛЬНЫЕ ДЕЙСТВИЯ ПРИ ПОЛУЧЕНИИ ЭЛЕКТРОННОГО ПИСЬМА:

При получении письма которое вызывает у Вас любопытство, чувство страха или побуждает к действиям: «открой», «прочитай», «ознакомься», в первую очередь **необходимо задуматься** и **задать себе** следующие **вопросы**:

- **ожидаю ли я это письмо?**
- **есть ли смысл в том, что от меня требуют?**
- **знаю ли я автора этого письма?**
- **уверен ли я в безопасности полученного электронного письма?**

Если ответ хотя бы на один из озвученных выше вопросов **«нет»** - внимательно проанализируйте содержимое письма и, при необходимости, свяжитесь для консультации с техническим специалистом.

ПЕРВОНАЧАЛЬНЫЕ ДЕЙСТВИЯ ПРИ ПОЛУЧЕНИИ ЭЛЕКТРОННОГО ПИСЬМА:

Особого внимания требуют письма, которые:

- **содержат ссылку** для перехода на сторонний ресурс (возможно, ссылка ведет на фишинговый поддельный ресурс);
- **содержат вложение** (возможно, файл содержит вредоносный код для заражения вашего компьютера);
- составлены **на иностранном языке**;
- **имеют большое количество получателей;**
- содержат **орфографические ошибки;**
- **связаны с финансовой, банковской сферой или геополитической обстановкой.**

КАК АНАЛИЗИРОВАТЬ ЭЛЕКТРОННЫЕ ПИСЬМА?

1. **Проверьте адрес отправителя** (*домен адреса электронной почты, с которой пришло письмо, должен совпадать с доменом, указанным на официальном сайте организации, от имени которой якобы направлено письмо, а логин такой почты, в свою очередь, должен совпадать с принятой логикой их построения в той или иной организации*). **Проверяйте адрес** отправителя**, даже в случае совпадения имени с** уже известным **контактом;**

2. **Проверьте полное имя отправителя** (*для проверки полного имени отправителя, наведите курсор мышки на указанное в письме имя отправителя*) и затем проанализируйте высветившийся адрес электронной почты в соответствии с информацией из официальных источников;

КАК АНАЛИЗИРОВАТЬ ЭЛЕКТРОННЫЕ ПИСЬМА?

3. **Проверьте**, при наличии, **ссылки**, даже если письмо получено от другого пользователя Вашей информационной системы, и **помните** о том, что сам **факт направления** Вам по электронной почте **ссылок**, ведущих на сторонний ресурс, **является подозрительным**:

- обратите внимание на название сайта, на который Вам предлагают перейти. В нем может быть изменен порядок букв или, например, некоторые буквы могут быть заменены на цифры (*например, www.s0branie.ru*);
- наведите курсор мышки на ссылку (*не нажимая на нее, ссылка появится или рядом с курсором или в левой нижней части окна*) и проверьте, чтобы URL, указанный в электронном сообщении, и URL, отображаемый при наведении курсора на ссылку, совпадали;
- также можно вручную (***не копируя ее***) вбить полученную ссылку в строке поисковой системы (Яндекс, mail.ru и др.). Такой метод позволит заметить возможные «**ошибки**» в полученной ссылке;

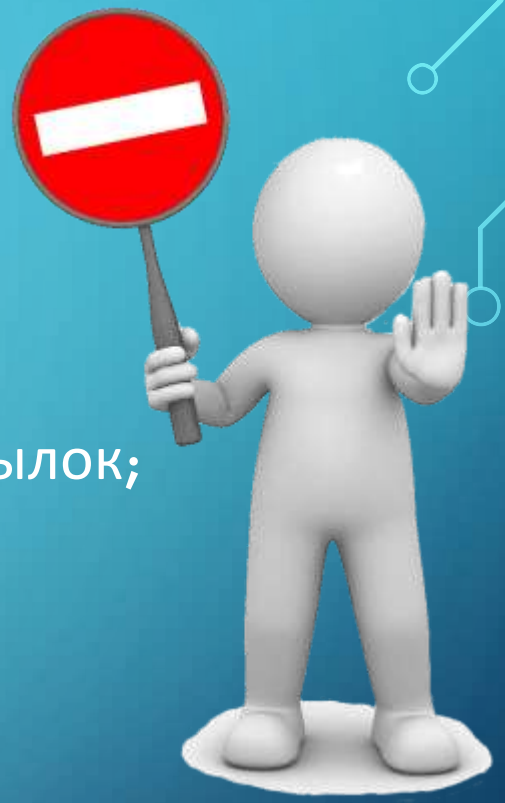
КАК АНАЛИЗИРОВАТЬ ЭЛЕКТРОННЫЕ ПИСЬМА?

4. **Проверьте наличие вложений**. Если отправитель, электронное письмо или причина, по которой Вас просят открыть вложение, вызывает **даже самое незначительное подозрение – ни при каких обстоятельствах не открывайте его**.

5. Обращайте внимание на возможные **опечатки, орфографические ошибки, большое количество прописных букв, совпадение названий организации, имени отправителя и содержимого** в тексте электронного письма;

6. Если полученное письмо вызывает **сомнения**, по возможности, **свяжитесь с отправителем или со справочной организации**, от которой пришло такое электронное письмо, **по другому каналу связи**. При этом **контактные данные** нужно **брать из авторитетных источников**, например, **на официальном сайте организации**, а не из направленного Вам письма.

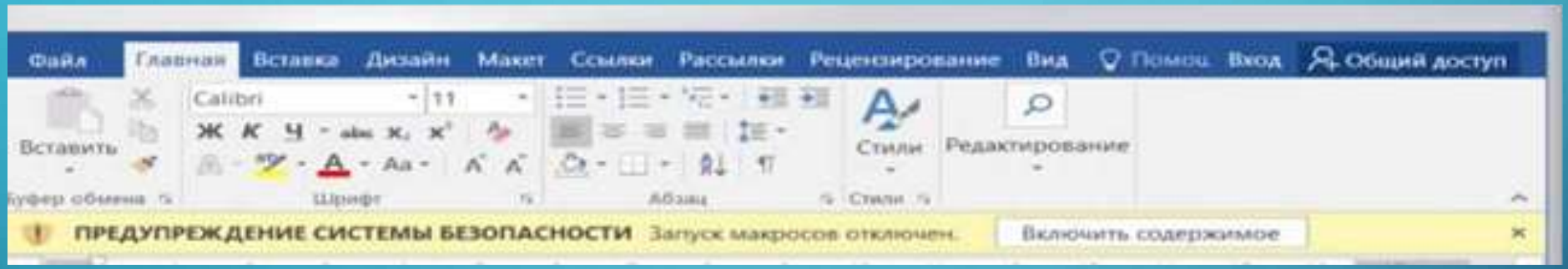
ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ОБНАРУЖИЛИ ФИШИНГОВОЕ ПИСЬМО?



1. **Не переходите по ссылке**, особенно, если они длинные или, наоборот, созданы при помощи сервисов сокращения ссылок;
2. **Не нажимайте на ссылки**, если они заменены на слова;
3. **Не копируйте адрес ссылки**;
4. **Не открывайте и не скачивайте вложения**, особенно, если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;
5. **Не подгружайте картинки** от незнакомых людей;

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ОБНАРУЖИЛИ ФИШИНГОВОЕ ПИСЬМО?

6. **Не запускайте макросы** в офисных приложениях (*макрос – это набор команд и инструкций, группируемых вместе в виде единой команды для автоматического выполнения задачи*);



7. **Не пересылайте письма** коллегам;

8. **Проинформируйте** технического специалиста/администратора информационной системы, направив ему полученное письмо как **«вложение»**;

9. **Удалите фишинговое письмо**.

СПАСИБО ЗА ВНИМАНИЕ!