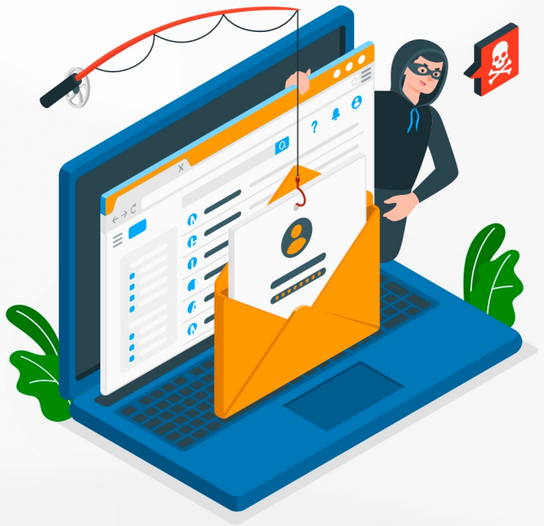
КАК НАС ЛОВЯТ НА КРЮЧОК?

Фишинг – это разновидность мошенничества, целью которого является получение паролей, банковских данных, конфиденциальной информации или заражения АРМ и серверов.

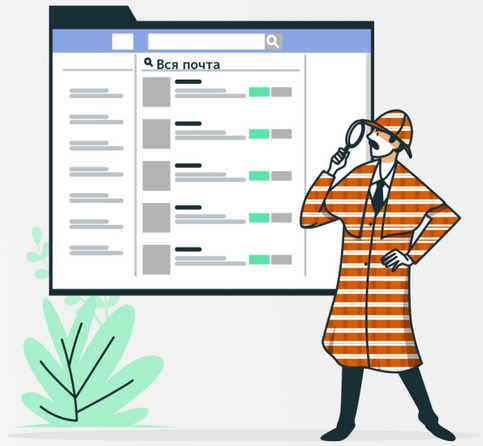


Злоумышленники массово рассылают электронные письма содержащие вредоносные вложения или ссылки на поддельные сайты новостных агентств, социальных сетей, банков или государственных органов.
Возможны варианты массовых мошеннических рассылок СМС или голосовых вызовов.

Отдельно выделяют целевой фишинг, когда рассылка готовится под определенную организацию или отрасль.

С фишинга начинаются большинство современных кибератак. Вас – пользователей корпоративных информационных систем, злоумышленники хотят обмануть, заставить запустить какой-то вредоносный файл или перейти на поддельный сайт.

Поэтому несмотря на применяемые в организации меры защиты несмотря на труд специалистов по защите информации в определенных ситуациях именно от пользователей, от их действий зависит – будет ли атака успешной и произойдет ли заражение.



Как распознать фишинг?

Мошенники стараются использовать Ваши слабости, для того чтобы достичь своих целей – получить информацию или побудить Вас сделать что-либо.

Слабости вызывают сильные эмоции (страх, гнев, любопытство и т.п.) и позволяют на секунду отключить критическое мышление.

Если вами пытаются манипулировать – скорее всего это мошенники.

Популярны рассылки от органов государственного контроля – ФНС, ЦБ РФ и других. Пользователи под страхом получения штрафов не задумываясь скачивают и запускают файлы, приходящие якобы от официальных лиц и с пометкой “срочно”.

При вводе логина, пароля или другой ценной информации на сайте убедитесь, что используется защищенное HTTPS соединение и действительный сертификат сайта – зеленый “замочек” слева от адреса сайта.

Всегда проверяйте какой настоящий адрес скрывается за ссылками в письме и на сайте. Для этого наведите мышку на ссылку в письме не нажимая её. В нижнем левом углу браузера вы увидите настоящий адрес сайта в сети Интернет.

Будьте осторожны и не переходите по необычным ссылкам во время работы в сети Интернет, не скачивайте файлы или не открывайте вложения электронной почты, если вы не уверены в их надежности.

Для проверки безопасности почтовых вложений, **обращайтесь в 185 отдел «Защиты информации»**, а установку нового программного обеспечения проводите только **при участии сотрудников отдела информационных технологий**.

ЦНИИ РТК

Отдел защиты информации – ib@rtc.ru – 4010 каб.
Сектор сетевой инфраструктуры – it@rtc.ru – 4035 каб.