Приложение
к письму Облкоминформтехнологии

ПАМЯТКА
пользователя по антифишингу

Антифишинг — одна из тактик интернет-мошенников, целью которой является попытка получения конфиденциальных данных. Для достижения данной цели злоумышленники выдают себя за известный пользователю источник, чтобы вынудить его передать им личную информацию (например, имя пользователя, пароль, данные банковской карты и пр.).

Получив эти данные, злоумышленники могут использовать их в своих целях (например, нанести финансовый, репутационный или иной ущерб пользователю, организации, в которой он работает, или третьему лицу).

Основной вид используемого злоумышленниками фишинга - почтовый фишинг с подменой сайта.

Злоумышленники отправляют пользователям письма под видом известного бренда: подделывают адрес, чтобы он напоминал официальный. Получатель нажимает на ссылку в письме и загружает вложение с вирусом, либо переходит на поддельный сайт и вводит там свои учетные данные.

Список часто встречающихся уловок для побуждения перехода по ссылке:

— Ваша учетная запись была или будет заблокирована/отключена.
— В Вашей учетной записи обнаружены подозрительные или мошеннические действия. Требуется обновление настроек безопасности.
— Вы получили важное сообщение. Перейдите в личный кабинет, чтобы ознакомиться.
— Фишинговые письма налоговой тематики.

Пример: пришло письмо от адреса gosuslugu.com@gmail.ru о том, что была попытка входа в Госуслуги и что необходимо срочно сменить пароль; пользователь, перейдя по ссылке из письма, на поддельном сайте вводит действующие учетные данные от Госуслуг, таким образом передавая их злоумышленникам.

Решение: всегда проверяйте адрес отправителя письма (в данном случае адрес отправителя должен быть no-reply@gosuslugi.ru), а также ссылку, по которой необходимо перейти в письме (официальный сайт Госуслуг – gosuslugi.ru). Обязательно проверяйте схожие символы (O-0, l-I

и др.). Если все же необходимо посетить ресурс, лучше введите его адрес вручную или воспользуйтесь ранее сохраненными закладками.

Фишинг может быть целевым. В этом случае мошенники нацеливаются на конкретную компанию, изучают нескольких сотрудников по аккаунтам в соцсетях или информации на сайте. Затем этим сотрудникам отправляют письма будто бы от коллег или руководителя: используют реальные имена, должности, номера рабочих телефонов. Пользователь думает, что получил внутренний запрос, и следует указаниям из письма.

Пример: пришло письмо от адреса grigoriev.i@mail.ru с просьбой произвести некоторые действия; пользователь выполняет данные действия и тем самым передает необходимые данные злоумышленникам.

Решение: всегда проверяйте адрес отправителя письма. Обязательно проверяйте схожие символы (O-0, l-I и др.). Свяжитесь другим способом с коллегой, который якобы отправил Вам письмо, и уточните у него, действительно ли он отправлял.

Как защититься от фишинга – общие правила

1. Обязательно проверяйте URL-адрес, по которому необходимо перейти, на наличие ошибок в написании. Обязательно проверяйте схожие символы (O-0, l-I и др.).
2. Используйте лишь безопасные https://-соединения. Отсутствие всего одной буквы “s” в адресе сайта должно обязательно насторожить.
3. С подозрением относитесь к любым письмам с вложениями и ссылками. Даже если они пришли со знакомого адреса, это не дает гарантии безопасности: он мог быть взломан. Не открывать вложения, не проверив перед этим его антивирусом.
4. Получив неожиданное подозрительное сообщение, если возможно, свяжитесь с отправителем каким-либо альтернативным способом и уточните, действительно ли он его послал.
5. Если все же необходимо посетить ресурс, лучше введите его адрес вручную или воспользуйтесь ранее сохраненными закладками. Не переходить по гиперссылкам из писем.
6. Не используйте для доступа к онлайн-банкингу и другим финансовым сервисам открытые Wi-Fi сети: часто их создают злоумышленники. Даже если это не так, подключиться к незащищенному соединению не составляет сложности для хакеров.
7. На всех аккаунтах, где это возможно, подключите двухфакторную аутентификацию. Эта мера может спасти положение, если основной пароль стал известен взломщикам.
8. Не сохраняйте в браузерах логин и пароль для входа на сайты или необходимые ресурсы.

Дополнительные материалы для изучения.

Раздел «Кибербезопасность – это просто!» на Едином портале государственных услуг – https://www.gosuslugi.ru/cybersecurity

Лендинговая страница в сети «Интернет» – https://киберзож.рф/