Таким образом, основные признаки фишинговых атак включают:

– неожиданные или подозрительные сообщения от отправителей, с которыми вы обычно не общаетесь;

– тексты, создающие атмосферу срочности или угрозы, требующие немедленных действий;

– подозрительные изменения в URL-адресах;

Ключевой момент в противодействии фишингу – сознательность и осведомленность пользователей интернета. Лаборатория Касперского дает следующие советы по противодействию фишингу:

1. Внимательно проверяйте электронные письма. Обратите внимание на следующие аспекты: 1) Броская тема письма. Мошенники часто пытаются привлечь внимание, манипулируя эмоциями жертвы, чаще всего жадностью или страхом. 2) Нагнетание обстановки. Такие фразы, как “немедленно!!!”, “у вас остался всего 1 час!!!” и избыток восклицательных знаков – уловки мошенников. 3) Наличие опечаток, ошибок и странных символов в тексте – попытка обойти спам-фильтры. 4) Странный адрес отправителя. Необычный адрес может служить признаком фишинга. 5) Ссылка в письме.

2. Не теряйте бдительность в мессенджерах и социальных сетях. Будьте скептичны по отношению ко всем ссылкам и рекламным баннерам.

3. Перед вводом номера карты остановитесь. Прежде чем вводить реквизиты карты задумайтесь, действительно ли вы находитесь на легитимном сайте. Обратите внимание на URL-адрес, проверьте наличие SSL-сертификата. Рекомендуется иметь отдельную карту для интернет-транзакций и пополнять её непосредственно перед оплатой. В случае утечки данных этой карты, потеря денежных средств будет незначительной.

4. Используйте разные пароли. Один и тот же пароль для всех учетных записей увеличивает риск их одновременной утраты в случае успешной фишинг атаки.

5. Включите двухфакторную аутентификацию для защиты аккаунтов. Наличие данной процедуры значительно усложняет злоумышленникам задачу по взлому вашего аккаунта.

6. Используйте надежную защиту. Наличие качественного антивируса – залог вашей безопасности в киберпространстве [1].

Литература

1. Как защититься от фишинга: 6 советов [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/blog/how-to-protect-yourself-from-phishing/31634/. – Дата доступа: 18.03.2024.

2. IT-безопасность для «ЧАЙНИКОВ» [Электронный ресурс, книга] / 2014. – Режим доступа: https://www.all-smety.ru/upload/iblock/ c9d/dummies_guide_it_security.pdf – Дата доступа: 16.03.2024

Т. Д. Запольский, Д. С. Сыч
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **А. В. Воруев**, канд. техн. наук, доцент

РЕАЛИЗАЦИЯ ПРИЛОЖЕНИЯ НА PYTHON ДЛЯ УПРАВЛЕНИЯ ПК С ПОМОЩЬЮ ГОЛОСОВЫХ КОМАНД

Голосовой ассистент – это программа, способная распознавать человеческую речь, реагировать и выполнять действия, соответствующие устному запросу пользователя. Созданная программа предназначена для работы с ПК, его программным обеспечением, подключёнными устройствами и программируемыми платформами независимо от того, каким образом они подключены: через порты или дистанционно.