Найбільш розповсюджені види сучасних комп'ютерних загроз

- ***шкідливе програмне забезпечення*** *(Malware)*
- ***інтернет-шахрайство***
- ***бот-мережі (bot-net)***
- ***крадіжка коштів***
- ***DDoS-атаки*** *(атаки на відмову в обслуговуванні)*
- ***«крадіжка особистості»*** *(Identity Theft)*

Шкідливе програмне забезпечення

Основні способи ураження:

-ураження комп'ютера під час відвідування шкідливого веб-сайту

- *повідомлення в соцмережі з посиланням на шкідливий сайт*
- *електронний лист з посиланням на шкідливий сайт*

-ураження при відкриті додатку до електронного листа з розширенням «.exe», «.bin», «.bat», «.dll», «.com», «.sys», «.scr».

Інтернет-шахрайство

*- **фішинг** (phishing)*

Атака полягає у спонуканні користувача ввести свої автентифікаційні дані (логін, пароль, банківську інформації) та іншу інформацію шляхом запевнення останніх щодо достовірності та справжності хибних (спеціально створених для цього) мережевих ресурсів (в тому числі просто посилань, за якими потрібно перейти), таких як пошта, веб-сайти, призначені для Інтернет-банкінгу, сторінки авторизації у соціальних мережах тощо;

*- **вішинг** (vishing)*

Вид шахрайства, що полягає в отриманні у користувача під час телефонної розмови, шляхом використання різних методів переконання, необхідної зловмиснику інформації. Один із різновидів «соціальної інженерії».

Бот-мережі *(bot-net)*

Сукупність комп'ютерів, уражених шкідливим програмним забезпеченням, ресурси несанкціоновано використовуються зловмисниками для різного роду незаконних дій (викрадення коштів, DDoS-атак, отримання персональных даних, шантажу і т.п.).

Крадіжка коштів

Використання можливостей несанкціонованого доступу до платіжних даних (реквізитів платіжних карток, паролів та ключів доступу до інтернет-банкінгу) або повного доступу до комп'ютеру (за рахунок його зараження шкідливим програмним забезпеченням) для проведення фінансових операцій.

DDoS-атака *(Distributed Denial of Service)*

Розподілена мережева атака, яка за допомогою численної кількості джерел має на меті порушити доступність сервісу (автоматизованої системи) шляхом вичерпання його обчислювальних ресурсів.

«Крадіжка особистості» *(Identity Theft)*

Несанкціоноване заволодіння персональними даними особи, що дозволяє зловмиснику здійснювати діяльність (підписувати документи, отримувати доступ до ресурсів, користуватися послугами тощо) від її імені ***(як один із механізмів підтвердження автентичності особи може використовуватись електронний цифровий підпис).***

Шахрайські електронні листи з посиланнями на віруси

1 вересня
5 вересня
9 вересня
10 вересня
15 вересня
22 вересня

Теми листів:

Від Міноборони України. Обов'язково для ознайомлення

ООО ГК «Содружество». Інформуємо Вас про виконання робіт

Государственная фискальная служба Украины, просим ознакомиться

Просим ознакомиться с документами, налог на недвижимость

Обязательно для ознакомления, документы

Высылаем Вам документы для проверки расчета НДС

Направляем Вам документы для проверки

Государственная фискальная служба, просим ознакомиться с документам

Шахрайські електронні листи з посиланнями на віруси

Міністерство оборони України
(Міноборони України)

Повітрофлотський, будинок 6
Україна, 03168, м. Київ
тел. (044) 280-31-06

Здравствуйтэ. Нагадуємо Вам, що у зв'язку з ситуації, що склалася, на південному сході України, просимо Вас уважно ознайомитися з цим документом(додаємо документ в листі) і звернути увагу на коментарі до кожного пункту. Невиконання умов, вказаних в документі, спричиняє за собою кримінальну відповідальність.
Додаток для розгляду:
1. Документація на 2 л. В 1 экз.

З глибокою повагою

генерал-лейтенант

В.В. Гелетей

_____

Прикладені документи:

Документація.doc
Скачать

Шахрайські електронні листи з посиланнями на віруси

Государственная налоговая служба

ул. Неглинная, д. 26

тел. (080) 271-03-41

Здравствуйте. Напоминаем Вам о том, что согласно ст. 265 НК, платить налог на недвижимое имущество, отличное от земельного участка, ежегодно обязаны физические и юридические лица, в том числе и нерезиденты, являющиеся собственниками объектов жилой недвижимости, просим Вас ознакомится с документами (прилагаются к письму) и принять соответствующие меры. В противном случаи Вас ожидают следующие неприятности:
1. По должникам материалы передаются судебным приставам для возбуждения судопроизводства и ареста имущества
2. Судебные приставы могут наложить арест на зарплатную карту либо на пенсионную карту
3. На сумму задолженности ежедневно растет пеня.

Приложение для рассмотрения:
1. Документ.rar на 2 л. В 1 эк

С глубоким уважением

ген. Директор

М. Н. Мишустин

Приложенные документы:

Документы.rar

Шахрайські електронні листи з посиланнями на віруси

Государственная фискальная служба Украины

Львовская пл., 8
Украина, 04655, Киев-53
тел. (044) 252-34-51

Приветствуем Вас. Напоминаем Вам, что согласно согласно ст. 265 НК, платить налог на недвижимое имущество, отличное от земельного участка, ежегодно обязаны физические и юридические лица, в том числе и нерезиденты, являющиеся собственниками объектов жилой недвижимости, просим Вас ознакомится с документами (прилагаем в письме) и принять соответствующие меры. В противном случаи Вас ожидают следующие неприятности:
1. По должникам материалы передаются судебным приставам для возбуждения судопроизводства и ареста имущества
2. Судебные приставы могут наложить арест на зарплатную карту либо на пенсионную карту
3. На сумму задолженности ежедневно растет пеня.

Приложение для рассмотрения:
1. Документ.rar на 2 л. В 1 э

С глубоким уважением

Государственная фискальная служба Украины

Приложенные документы:

Документы.rar

Основні рекомендації щодо забезпечення інформаційної безпеки

*Слідкувати за **оновленням** операційної системи та іншого програмного забезпечення, що використовується.*

*Користуватися **легальним антивірусним** програмним забезпеченням та регулярно оновлювати бази даних сигнатур вірусів.*

*Використовувати програмний міжмережевий екран (**брандмауер**) та штатні засоби захисту від шкідливого програмного забезпечення.*

При користуванні послугами Інтернет-банкінгу, електронної пошти тощо, у разі необхідності введення автентифікаційних даних впевнитись у тому, що використовується ***захищене з'єднання HTTPS.***

Бути уважним до проявів ***Інтернет-шахрайства****. Особливу увагу варто звертати на доменне ім'я Інтернет ресурсу, що запитує автентичні дані. В іншому випадку є велика ймовірність перейти на фішингову сторінку, зовні ідентичну справжній, та самостійно «віддати» власні автентичні дані.*

При користуванні Інтернет-ресурсами (соціальні мережі, системи обміну повідомленнями, новини, онлайн-ігри) не переходити по невідомих посиланнях та не завантажувати файли, що мають потенційно ***небезпечне розширення*** *(наприклад, .exe, .bin, .ini, .dll, .com, .sys, .bat тощо).*

Систематичне ***підвищення рівня обізнаності*** *з питань безпечного використання інформаційних технологій та протидії загрозам.*