Hack to Learn – Spam, Spoofing and Phishing

Spam

Email spam, also known as junk email means nearly identical messages sent to numerous recipients by email. Clicking on links in spam email may send users to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments. You should not open (double-click on) attachments in spam email!

The legal status of spam varies from one jurisdiction to another. In the United States, spam was declared to be legal by the CAN-SPAM Act of 2003 provided the message adheres to certain specifications.

Spoofing

E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations. Spoofing can be used legitimately.

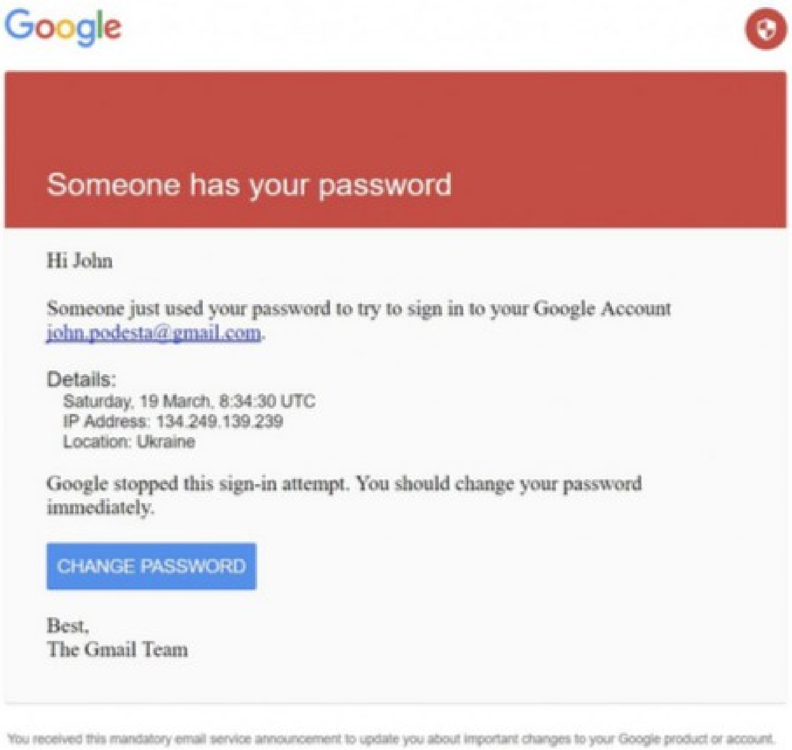
E-mail spoofing is possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending e-mail, does not include an authentication mechanism. Although an SMTP service extension (specified in IETF RFC 2554) allows an SMTP client to negotiate a security level with a mail server, this precaution is not often taken. If the precaution is not taken, anyone with the requisite knowledge can connect to the server and use it to send messages. To send spoofed e-mail, senders insert commands in headers that will alter message information. It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say. Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write.

In October 2013, an e-mail which looked like it was from the Swedish company Fingerprint Cards was sent to a news agency, saying that Samsung offered to purchase the company. The news spread and the stock exchange rate surged by 50%. It was later discovered the e-mail was a fake.

Phishing

Suppose you check your e-mail one day and find a message from your bank. You've gotten e-mail from them before, but this one seems suspicious, especially since it threatens to close your account if you don't reply immediately. What do you do?

This message and others like it are examples of **phishing**, a method of online identity theft. In addition to stealing personal and financial data, phishers can infect computers with viruses and convince people to participate unwittingly in money laundering.



Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.

- John Podesta, H. Clinton’s campaign chairman, received this legitimately looking email on March 19, 2016.
- Mr. Podesta clicked on the blue “change password” button, which took him to a website owned by Fancy Bear, a group of hackers.
- In October 2016 Wikileaks started releasing thousands of Podesta’s emails, with detrimental consequences to H.Clinton’s election campaign.
- Colin Powell’s account was hacked in the exact same fashion, by the same group in the past.

Exercise

```
import smtplib
def send_phishing_email(from_addr, to_addr_list, cc_addr_list,
              subject, message,
              login, password,
              smtpserver='mail.schoolnova.org:26'):
    header  = 'From: barack.obama@whitehouse.gov\n'
    header += 'To: %s\n' % ','.join(to_addr_list)
    header += 'Cc: %s\n' % ','.join(cc_addr_list)
    header += 'Subject: %s\n\n' % subject
    message = header + message
    server = smtplib.SMTP(smtpserver)
    server.starttls()
    server.login(login,password)
    problems = server.sendmail(from_addr, to_addr_list, message)
    server.quit()
    return problems
print ("Start sending mail")
results = send_phishing_email(from_addr    = 'itta@schoolnova.org',
          to_addr_list = ['<to email address>'],
          cc_addr_list = [],
          subject      = 'The president invites you to his Facebook',
          message      = 'Click here for Barak Obama Facebook page',
          login        = 'it102@schoolnova.org',
          password     = 'test102!')
if (len(results)):
    print(results)
print ("Finished sending mail")
```

Documentation: https://docs.python.org/3/library/smtplib.html

Homework

1. Add a Facebook logo, fonts and colors to your email message;

2. Put the email sending function call in a loop, so that it sends 2 or 3 emails;

3. Note that the it102@schoolnova.org account will be disabled by next week.