How I stopped worrying and love the SPAM

I have a new hobby. It's called phishing.

I send fake banking e-mails to gullible executives, then I find out their financial information and use it to steal the money they don't deserve.

Dear Customer,
This is your bank. We forgot your social security number and password. Why don't you send them to us so we can protect your money.
Sincerely,
I. B. Banker

Robin A. Gandhi
Nebraska University Center on Information Assurance (NUCIA)
College of Information Science and Technology (IS&T)
University of Nebraska at Omaha (UNO)
NUCIA
Nebraska University Center for Information Assurance
http://nucia.ist.unomaha.edu/
The NUCIA Team

Ken Dick
Robin Gandhi
Matt Hale
Ryan Schuetzler
Bill Mahoney
Chris Daniels
Abhishek Parakh
Leah Pietron

5/4/17
NUCIA

• NSA/DHS designated Center of Academic Excellence in Information Assurance Education

• Degrees include
  – Bachelors in Cybersecurity; Masters in Cybersecurity, Cybersecurity concentrations for MS in CS and MIS, PhD in IT
  – Non-degree programs and activities include
    • Certificates, IT professionals academy
    • Special programs for High School teachers and students
.NULLify Presents:

HIGH SCHOOL CTF: RETRO

HSCCTF will be on November 19th and hosted at the Nebraska Ballroom on the University of Nebraska Omaha campus.

CTF:Retro has ended!

http://ctf.nullify.uno
NATO Lock Shields

Locked Shields is a real-time network defence exercise, organised annually since 2010 by the NATO Cooperative Cyber Defence Centre of Excellence. The Estonian Cyber Range forms the backbone of the game-based exercise, with new attack vectors and technologies being introduced every year, in sync with market developments.

16 nations and NATO Computer Incident Response Capability participated as the Blue Teams of Locked Shields 2015. A total of 400 people were involved in the exercise. The training audience of the exercise were the national Blue Teams: computer emergency response specialists, playing the role of the rapid reaction teams of the fictional country of Berlya. The team from NATO Computer Incident Response Capability (NCIRC) came out as a winner, Estonia and Poland took second and third place respectively.

The largest of its kind globally, Locked Shields is unique in using realistic technologies, networks and attack methods. In 2015, new attack vectors included ICS/SCADA systems and Windows 8 and 10 operating systems, as well as an element of active defence. In addition to technical and forensic challenges, Locked Shields also includes media and legal injects. It thus provides insight into how complex a modern cyber defence crisis can be, and what is required from nations in order to be able to cope with these threats.

Locked Shields 2015 was supported by the Government of Canada. The grant covered purchase of technical equipment for the NATO Cooperative Cyber Defence Centre of Excellence cyber lab and supporting services that allowed to increase the capacity of the annual Locked Shields cyber defence exercise.
My own achievement! Or is it?

barack.obama@whitehouse.gov
To: Robin Gandhi <rgandhi@unomaha.edu>
RE: Research

Dr. Gandhi,
Congratulations on your most recent achievements in your research. Please refer to the below URL to review your funding request.

Grant f
Yours truly,
Barack
President

barack.obama@whitehouse.gov
To: Robin Gandhi <rgandhi@unomaha.edu>
RE: Research
Why worry about scams in the digital age?

As if we did not have enough to worry about....
scam
/skam/  ➦
	noun informal

1. a dishonest scheme; a fraud.
   "an insurance scam"
   synonyms: fraud, swindle, fraudulent scheme, racket, trick; More pharming;
   informal con, hustle, flimflam, bunco, grift, gyp, shakedown
   "the scam involved a series of bogus investment deals"

verb

1. swindle.
   "a guy that scams the elderly out of their savings"
   synonyms: swindle, cheat, deceive, trick, dupe, hoodwink, double-cross, gull; More
   informal rip off, con, fleece, shaft, hose, sting, bilk, diddle, rook, gyp, finagle, bamboozle, flimflam, put one over on, pull a fast one on, sucker, stiff, shake down, hornswoggle
   "he was trying to scam residents with phony insurance policies"

Translations, word origin, and more definitions
Stranger Danger!
1. **Distraction Principle**
   While we are distracted by what grabs our interest, hustlers can do anything to us and we won’t notice. (Stajano 71)

2. **Social Compliance Principle**
   Society trains people to not question authority. Hustlers exploit this “suspension of suspiciousness” to make us do what they want. (Stajano 72)

3. **Herd Principle**
   Even suspicious marks let their guard down when everyone around them appears to share the same risks. Safety in numbers? Not if they’re all conspiring against us. (Stajano 73)

4. **Time Principle**
   When under time pressure to make an important choice, we use a different decision strategy, and hustlers steer us toward one involving less reasoning. (Stajano 73)
156 Million Phishing Emails (Every Day)
140 Million
Crash and burn at spam filters

ARRun it’s the googles
But that means…
16 Million
Make it through Filters

8 Million
are actually opened

CHARRRRRRRRGE
I have you now

800,000 Links are clicked

NOT ALTERNATIVE FACTS
80,000
Fall for a scam and/or share their personal info.

Grandma
Uncle Ed.
You?

Awesome Pirate graphics courtesy Canadian PSA and Matt Hale for finding it:
Phishing affects us all and drains around 6 billion annually from world economies.
Clearly need more than spam filters...
Mining Information

What does Maltego do?

- Maltego is a program that can be used to determine:
  - People
  - Groups of people (social networks)
  - Companies
  - Organizations
  - Web sites
  - Internet infrastructure such as:
    - Domains
    - DNS names
    - Netblocks
    - IP addresses
  - Phrases
  - Affiliations
  - Documents and files
- These entities are linked using open source intelligence.

FBStalker: https://www.youtube.com/watch?v=g6sOi9FOz2o
Search By

First  Robin
Last   Gandhi

Results for Robin Gandhi, Nebraska, United States

Robin Amrit Gandhi
37 years old from Nebraska
Assistant Professor at The University of Nebraska, Omaha

Robin A Gandhi
Elk Horn, Nebraska

Robin A Gandhi
Elkhorn, Nebraska
Ask and you shall receive

https://www.trustedsec.com/social-engineer-toolkit/

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailor Attack
6) Arduino-Based Attack Vector
7) SMS Spoiling Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules

set> Return back to the main menu.
The Line to get into DEFCON at Las Vegas 26
Email headers

• Typical Email Display
  – Where is the header (real one)?
The “Real” Header (3-clicks away)

Please refer to the below URL to review Grant funding request.
Yours truly,
Look for the last "Received" header from the top.

```
Received: from loki.ist.unomaha.edu (localhost [127.0.0.1])
   by loki.ist.unomaha.edu (Postfix) with ESMTP id DC7C51E0577
   for <rgandhi@unomaha.edu>; Mon, 9 Dec 2013 21:53:15 -0600 (CST)
```
network-tools.com

Domain Name: UNOMAHA.EDU

Registrant:
University of Nebraska at Omaha
60th and Dodge Street
Omaha, NE 68182-0051
UNITED STATES

Administrative Contact:
UNO IS
Abuse reports to http://abuse.unomaha.edu
University of Nebraska at Omaha
60th and Dodge Street
Omaha, NE 68182-0051
UNITED STATES
1-402-554-4357
[email protected]
What can you do?
<table>
<thead>
<tr>
<th>MessageId</th>
<th><a href="mailto:933a18dd-40b1-4ec3-be7a-f4b99c64f7eb@BY2NAM01FT010.eop-nam01.prod.protection.outlook.com">933a18dd-40b1-4ec3-be7a-f4b99c64f7eb@BY2NAM01FT010.eop-nam01.prod.protection.outlook.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Created at</td>
<td>8/5/2016, 4:20:09 AM (Delivered after 6 sec)</td>
</tr>
<tr>
<td>From</td>
<td>Google Incorporation <a href="mailto:incoming@julia.net">incoming@julia.net</a></td>
</tr>
<tr>
<td>To</td>
<td><a href="mailto:rgandhi@unomaha.edu">rgandhi@unomaha.edu</a></td>
</tr>
<tr>
<td>Subject</td>
<td>Google-Lottery-result-announcement(<a href="mailto:rgandhi@unomaha.edu">rgandhi@unomaha.edu</a>)</td>
</tr>
<tr>
<td>SPF</td>
<td>none</td>
</tr>
<tr>
<td>DKIM</td>
<td>none</td>
</tr>
<tr>
<td>DMARC</td>
<td>none</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Delay</th>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Time received</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2 sec</td>
<td>BY2NAM01FT010.eop-nam01.prod.protection.outlook.com</td>
<td>SN1PR0701CA0021.outlook.office365.com</td>
<td></td>
<td>8/5/2016, 4:20:15 AM</td>
</tr>
</tbody>
</table>
Reading a URL


http://www.buy.com.money.ru

http://www.facebook.sozial.com/login.asp
Phishing Links

https://goo.gl/AWatvP
Reading a URL

• Which link would you click?


Robin A. Gandhi, Ph.D.
Charles & Margre Durham Associate Professor
School of Interdisciplinary Informatics, Cybersecurity

PKI 177A
6001 Dodge Street
Omaha, NE 68182

PH : 402-554-3363
FX : 402-554-3284
rgandhi@unomaha.edu
Project Goals

- Catalog datasets and build common schemas for innovations in Bridge Health
- Identify opportunities with big data technologies for bridge health monitoring
- Address challenges of data discovery and controlled sharing
- Transition bridge health monitoring data into pipelines for data science

Current Accomplishments

- Bridging Big Data 2016 Workshop, Omaha
  - Follow-up from a self-funded 2015 workshop
- Upcoming: Bridging Big Data 2017, Omaha
  - Co-located with MBDH All-hands Meeting, Oct 4, 2017
  - Researchers from UNO and UNL are engaged with project partners for research in this emerging area
    - Pilot projects with government agencies, industry and academic partners are underway

https://bridgingbigdata.github.io
http://engineering.unl.edu/bridging-big-data-workshop/