Beyond the Nigerian Prince: The Evolution of Phishing & How We Fight Against It

November 1, 2018
Logistics

> You will be on mute

> Submit questions in the Q&A box (probably on the right side of your screen) in the GoToWebinar control pane

> Webinar is being recorded and will be available for replay

> Slides will be made available after the webinar
Tim’s story
“I thought we’d solved the phishing problem.”
### Which Threats Bypass Email Security Solutions?

<table>
<thead>
<tr>
<th>Threat Description</th>
<th>Email Security Professionals</th>
<th>Lay People</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impersonation of an executive, other internal employee, or external person</td>
<td>63.5%</td>
<td>17.5%</td>
</tr>
<tr>
<td>(e.g. business partner, customer, vendor, etc)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business services spoofing (e.g. DocuSign, ADP, UPS)</td>
<td>42%</td>
<td>20.2%</td>
</tr>
<tr>
<td>Wire transfer request</td>
<td>38.7%</td>
<td>5.3%</td>
</tr>
<tr>
<td>Credential theft (e.g. sending you to a fake login page)</td>
<td>34.3%</td>
<td>12.3%</td>
</tr>
<tr>
<td>Payload attacks (e.g. malicious / suspicious attachments or links)</td>
<td>33.1%</td>
<td>12.3%</td>
</tr>
<tr>
<td>W2 or confidential information requests</td>
<td>21.5%</td>
<td>7%</td>
</tr>
<tr>
<td>None of the above or Nothing but Spam</td>
<td>15.5%</td>
<td>66.1%</td>
</tr>
</tbody>
</table>

1 in 5 have to take direct remediation action at least weekly.
Email Security: A Shared Responsibility

Prevention
Industry

Protection
Organization

Individual
Evolution of Email Security Risk

Time
Way Back When...

Waves of spam

Spam wave #1

Spam wave #2

Spam wave #3

Spam wave #4
Way Back When...

Waves of spam

1. Collect as much spam & ham as possible.
2. Find patterns that match against spam waves.
3. Block spam.
4. Do it best = $$$
Volumetric Phishing

URGENT!!! MV DANLIANG V23 Enquiry for taking bunker + PDA

HongFa Shipping Co., Ltd <wurong@hongfshipping.com>

Wednesday, September 26, 2018 at 6:44 AM

Show Details

This message appears to be junk mail. Beware of links in this message.

Dear Sir

Good day!

Pls urgently help to check/advise if the above mentioned vessel can take bunker at anchorage? and the PDA of bunkering there

Vessel's particulars and information as attached below:

Thanks and best regards

吴嵘
Rick Wu
Manager of document dept
Shipping Div.
HongFa Shipping Co., Ltd
Tel: +86-21-66293090(direct) or +86-21-66293121-3090
Fax: +86-21-63373408
Cell: +86-18818009776
E-mail: wurong@hongfshipping.com
www.hongfshipping.com

---

Urgent respond

This message appears to be junk mail. Beware of links in this message.

Hi, I am miss Elizabeth Nelson 25 years old lady i have every important things to discuss with you. please respond to my email to enable me give you the brief details of prosper. Kindly email me on nelsonelizabeth457@gmail.com, Looking forward for your positive response. Best Regards Elizabeth.
Uh Oh...
Spear Phishing

From: Kevin O’Brien <pad@remotemail.me>
Sent: Tuesday, October 23, 2018 10:14 AM
To: Chris Wade
Subject: Urgent Request

I am in a meeting. You available at the office now? Respond to my email.

Sent from my iPad

---

Kevin O. <earljordan114@gmail.com>
Lorita Ba

Tuesday, October 23, 2018 at 10:38 AM

Show Details

Got a minute? I need you to complete a task for me as soon as possible.
P.S.: I am in a meeting now and can’t talk, so just reply back.

Regards.
--
Sent from my iPad

---

We have been working on acquiring a company in the tech space – we are (finally) wrapping up. I have asked Greg from Foley Hoag to get in contact with you; we need to tie up a few outstanding accounting details for the M&A filing.

In addition the standard corporate governance information, he will be sending transactional information to finalize the acquisition itself. You have my full approval to process with any of his requests.

This is obviously bound by SEC regulations, and we are in the mandatory quiet period. Please keep the matter strictly confidential until we publicly announce it.
Consider More Than Just Technology

Processes

Technology

People

Organization

Individual

Industry, Organization
Strengthen Email Security Efforts with User Engagement

Legacy Way
> Mitigate user risk (Quarantine, quarantine, quarantine)

Modern Approach
> Provide end users with the context and tools they need to positively contribute to email security efforts

This may be a phishing attempt. Justin Anderson does not typically send from anderjus@gmail.com. Be careful interacting with the content in this email.
Build Out Business Processes to Mitigate Common Attack Vectors

**Legacy Way**
- **Rely** on technology and security awareness training to catch 100% of threats

**Modern Approach**
- **Use** technology and in-context security training to enforce policies that mitigate risk
Establish a Trusted Online Presence

**Legacy Way**
- Focus on website security and firewall/perimeter based defenses

**Modern Approach**
- Deploy internet-wide tools and standards to establish trust
Continue Efforts Across the Entire Spectrum
Control your email with DMARC. Control your DMARC process with dmarcian.

*dmarcian* specializes in processing complex DMARC reports and identifying what steps need to be taken, so you can become DMARC compliant.

At *dmarcian*, we see email security and authentication as cornerstones of the Internet. We’re dedicated to upgrading the entire world’s email by making DMARC accessible to all. *dmarcian* brings together thousands of senders, vendors, and operators in a common effort to build DMARC into the email ecosystem.

We believe email is worth fixing.

GreatHorn simplifies email security by automating detection, remediation, and incident response.

Security teams using GreatHorn not only gain enterprise-class protection against both sophisticated phishing attacks and traditional threats, they also reduce complexity, manual remediation time, and negative impact on business operations.
Questions?

> Recording and slides will be made available following the webinar

> Keep an eye out for our upcoming webinars (dates TBD):

  - **A How-To Guide to Modernizing Your Phishing Defenses**
    (Part 2 in our “Beyond the Nigerian Prince” series)

  - **Comprehensive Phishing Defense with dmarcian and GreatHorn**
    (Part 3 in our “Beyond the Nigerian Prince” series)