Simulated Phishing

Simulated Phishing

In order to raise awareness of current phishing attack tactics, the Berkeley Lab Cyber Security team sends emails to Berkeley Lab employees that simulate real phishing attacks. If you would like to help improve Berkeley Lab's phishing awareness please sign up below.

The goal of this simulated phishing campaign is to help you to learn how to spot a phish and report it to the Cyber Security team. Accurately reporting phishing allows the Cyber Security team to alert other employees and block future phishes.

Sign up

Simulated phishing emails will be sent only to users that have filled out this.

What is Phishing?

An important part of this campaign is distinguishing between what is a phishing email, a targeted phishing email, and spam.

<table>
<thead>
<tr>
<th>Attack</th>
<th>Description</th>
<th>Action you should take</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted Phishing</td>
<td>A phishing attack that targets your affiliation with Berkeley Lab, UCB, or DOE to steal sensitive data (passwords, SSNs, etc). These messages could appear to come from LBL email addresses or reference Lab employees.</td>
<td>Report immediately to <a href="mailto:security@lbl.gov">security@lbl.gov</a></td>
</tr>
<tr>
<td>Phishing</td>
<td>Attacks that are carried out in order to steal passwords, SSNs, and other sensitive data. These messages often ask you to click on a link, send information, or enter credentials by pretending to be a credible website (such as a bank).</td>
<td>Report to <a href="mailto:security@lbl.gov">security@lbl.gov</a></td>
</tr>
<tr>
<td>Spam</td>
<td>These are unwanted messages but are not asking for sensitive information.</td>
<td>Good to update spam filters by using our</td>
</tr>
</tbody>
</table>

How do I report a phishing email?

Send an email to security@lbl.gov reporting the incident and include the source code of the phishing email as an attachment. If you do not know how to attach the source code click here to learn how to forward the source code of an email as an attachment:

FAQ

I think I received a simulated phish, what should I do with it?

Please report simulated phishing just as you real phishing, by either using the Chrome Phishme Reporter extension or by forwarding to security@lbl.gov

Privacy

Information about individual responses will NOT be shared with anyone outside the security team. Passwords will NOT be stored. This information will never be used or released in any identifiable manner outside the security group, including in any manner which would be used to evaluate your job performance. Simulated phishing is designed as a training exercise and to help the Laboratory understand our overall exposure to phishing as well as to target our protections and training. It is in no way designed and will not be used to judge the performance of individuals.

Feedback

In order to improve this program please fill out this form after receiving a simulated phishing email:
Past Simulated Phishing Campaigns

Below are screenshots of the simulated phishing campaigns that have been run so far at LBNL.

#5 2017-10-16: FY17 Performance Review Problem

This email was intended to get users to question the legitimacy of the pdf attachment even though the sender appears to have a "real" lbl.gov email address. The attachment link in the email directed to a spoofed google login page in order to retrieve the username and password of the user. The fake employee Brian Schick was created to demonstrate the situation where an email address is spoofed or compromised. Emails sent to Brian was answered by the security group.

Users were expected check for Brian Schick on the directory as well as notice they were being asked to log in with LBL credentials to a non-LBL site.

Sender: Brian Schick - bschick@lbl.gov

Link: http://downloads.careerpost.us/

The Email:

FY17 Performance Review Problem

Brian Schick bschick@lbl.gov via return--path.com

to me ▼

Review the attached problem with your FY17 Performance Review.

Thank you,
--Brian--

The Landing Page:
Sign in with your Account.

Enter your email

Next

Find my account

Create account

The Education Page:
Look below to see the suspicious indicators of this phishing email

This email was intended to get users to question the request to input credentials into a non-LBL site. The link in the email directed to a non-LBL login page in order to tempt users to enter passwords. The fake employee Ingrid Peters was reused from the previous phish. Ingrid was added to the user directory to demonstrate the situation where an email address is spoofed or compromised. A phone number was added to Ingrid’s directory entry that would be answered by security group.

Users were expected to notice that they were being asked to log in with LBL credentials to a non-LBL site as well as notice the reuse of the ipeters@lbl.gov address.

Sender: Ingrid Peters - ipeters@lbl.gov

Link: http://login.securefilesshares.com

The Email:
Your employee evaluation has been updated

Ingrid Peters via return-path.com
to me

Dear Arthur:

Here at LBNL we take employee performance very seriously. As part of a new initiative, we have asked management to conduct routine evaluations of all employees in the Information Technology department. Your supervisor has uploaded your most recent evaluation. Please login to our secure portal using your LBNL username and password.

Thank you,

Ingrid Peters
Human Resources

The Landing Page:

Secure File Shares

The most secure file sharing service the cloud has to offer!

Username: 
Password: 
Log In

To access shared files, please use the username and password provided by your organization.

The Education Page:
This email was intended to get users to focus on the URL despite the use of a "real" lbl.gov email address. The link in the email directed to a fake LBL login page in order to tempt users to enter passwords. The fake employee Ingrid Peters was added to the user directory to demonstrate the situation where an email address is spoofed or compromised. A phone number was added to Ingrid's directory entry that would be answered by security group.

Users were expected to notice the non-LBL link that the email directed to or to call the number for Ingrid Peters to check the validity of the email out-of-band.

Sender: Ingrid Peters - ipeters@lbl.gov

Link: http://www.lbl.gov.hr-communication.com/

The Email:
Hi Arthur,

The 2016 W-2 (Wage & Tax Statement) will be mailed to your home address on Jan 31, 2017. Unfortunately, we no longer have your address on file. Go here to update your address. For international address changes, contact your HR Center business partner.

Thank you,
Ingrid Peters
Human Resources

The Landing Page:

[Image of login page with the URL www.lbl.gov/hr-communication.com/?login_id=39efa8ce-f7bd-4194-8]

The Education Page:
Look below to see the suspicious indicators of this phishing email

This email was intended to get users to focus on the URL and demonstrate that it is often trivial to make an email or web site that looks like ones you trust. It mimicked the HTML of a real "Invitation to Edit" email sent by Google Drive as well as the LBL login page. The email appeared to be from an LBL employee (although this user doesn’t exist).

Users were expected to notice the non-LBL link that the email directed to or check the existence of the sender.

Sender: fzuidema@lbl.gov - Frank Zuidema

Link: http://lbl.gov.invoicenotices.com

The Email:
The Landing Page:

Secure File Shares

The most secure file sharing service the cloud has to offer!

Username: 
Password: 
Log In

To access shared files, please use the username and password provided by your organization.

The Education Page:
This email was our first phish and intended to test the waters. It emulated the common phishing emails that are vague, urgent, and not necessarily relevant. It had an fake sender address that appeared to be from within LBNL.

Sender: compmaint@lbl.gov - Computer Maintenance

Link: http://lbl.gov.webaccess-alerts.net/

The Email:
Urgent: Email reactivation

Computer Maintenance via return--path.com
to me

Jay Krous,

You are required to upgrade mail quota within 48 hours to maintain normal email delivery.

Click here to log in.

Thank you,
Computer Maintenance Team

The Education Page:

Look below to see the suspicious indicators of this phishing email

Note vague and urgent language of the subject

Hover over the link to see lbl.gov.webaccess-alerts.net
That is not a Lab domain

This is no assurance it's really from the Lab.

Click here to provide feedback on this simulated phishing campaign.