

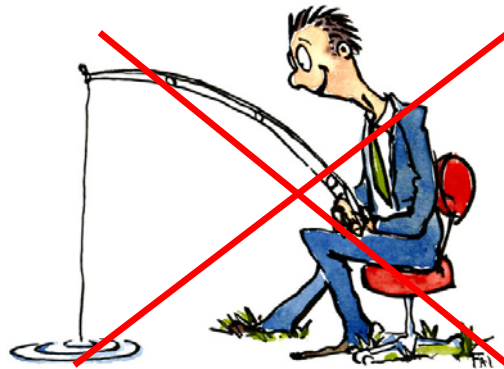


# Lucas County Anti-Phishing Training

How to "Spot the Phish"

# What is a Phishing Attack?

Phishing: Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.





# Lucas County Phishing Test

- Lucas County Information Services conducted a phishing test for email users in August 2019.
- Email was delivered, data compiled and the results are in.



# The Send

**From:** IT <IT@co.lucas.oh.us>  
**Reply-to:** IT <IT@co.lucas.oh.us>  
**Subject:** Password Check Required Immediately

**Template ID:** 77738-199477  
[Send me a test email](#)  
[Toggle Red Flags](#)

To All Employees,

As part of ongoing efforts to maintain regulatory compliance we have updated our password policy and we need everyone to check their password immediately.

Please click here to do that:

[Check Password](#)

Please do this right away.

Thanks!

Mail From: IT <IT@co.lucas.oh.us>

File Edit View Actions Tools Window Help

Close Reply Reply All Forward

Mail | Properties | Message Source | Discussion Thread

IT <IT@co.lucas.oh.us> 8/21/2019 2:05 PM

Password Check Required Immediately

to: Julie Riley

GroupWise has prevented images on this page from displaying. Click here to display images

To All Employees,

As part of ongoing efforts to maintain regulatory compliance we have updated our password policy and we need everyone to check their password immediately.

Please click here to do that:

[Check Password](#)

Please do this right away.



Thanks!

<http://guru.phishing.guru/XcmVajaXBpZWR50X2IkPTaQ5NDM2TUMDA5HMCZjYW1wqYWfInbl9ydW5>

<http://guru.phishing.guru/XcmVajaXBpZWR50X2IkPTaQ5NDM2TUMDA5HMCZjYW1wqYWfInbl9ydW5faWQ9Mjl5AMjA1NSZhY3Rpb249Y2xpY2smdXJsPW50dl>

# The Redirect after Clicking



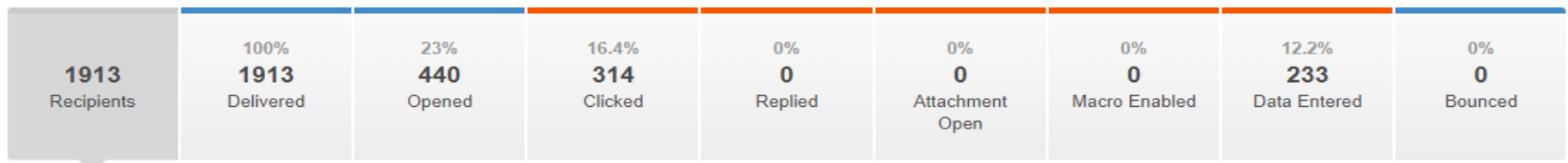
User Name / E-mail Address	
Password	

Check Password

This page is compliant with HTML5 for cross-browser and mobile support.

This page is intended for Lucas County employees ONLY!

# Results At a Glance



⚙ This Phishing Security Test	
STATUS	Closed
PHISH PRONE	28.6%
RECIPIENTS	1913
FAILURES	547
CAMPAIGN END	08/27/2019 10:55 AM

- 1913 emails were delivered
- 547 users failed the phish
- Counts double against users who entered Data, not just clicked
- 28.6% of 1913 users are phish prone
- Industry Average: 10.8%

# Important Numbers

23%  
**440**  
Opened

- 23 % of all users opened the Phishing Email.

16.4%  
**314**  
Clicked

- 71.4 % of those who opened the email, clicked the link.

12.2%  
**233**  
Data Entered

- 74.2 % of those who clicked the link, submitted their data.



# What Are Consequences of a Phishing Attack?

**Virus:** A type of malicious code or program written to alter the way a computer operates and to spread itself from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

**Unauthorized Network Access:** When someone gains access to a website, program, server, service, or other system using someone else's account or other methods.

# What Are Consequences of a Phishing Attack?

**Email Interception or Fabrication:** The practice of monitoring the internet to read private messages that were intended for other people.

**Password Theft:** Various measures used to discover computer passwords. This is usually accomplished by recovering passwords from data stored in, or transported from a computer system.

**Ransomware:** A form of malicious software-malware-that encrypts documents on a PC or even across a network. Victims can often only regain access to their encrypted files and PCs by paying a ransom to the criminals behind the ransomware.

# How to Spot Phishing Emails

Asking for personal information	Most reputable organizations won't ask for personal information in an email.
Inconsistent or Suspicious Links	Hover over links with your mouse to display the full URL. If it doesn't seem to belong— don't click!
Unrealistic Threats or Sense of Urgency	Phishing emails often add threats to get you to panic and react.
Asking to Send Money	Any email asking for you to send money should immediately raise concerns.
Poor Spelling and Grammar	Most generic phishing attempts contain spelling, grammar errors or awkward wording/phrasing.
Suspicious Attachments	Take caution with unexpected attachments.
If in Doubt – Throw it out!	Even if you think you know the source, if something looks suspicious, delete it or send it to LCIS for review.

## What To Do if a Suspected Email Arrives in Your Inbox

- Don't open the email. Should you open the email to read the contents do not click on any links provided.
- Call or forward suspected email *as an attachment* to LCIS Helpdesk [lcishelpdesk@co.lucas.oh.us](mailto:lcishelpdesk@co.lucas.oh.us).
- Inform others in your office of the email.
- Move the email to your junk mail or spam folder.

# Phishing Email Examples

The screenshot shows an email interface with a header bar. On the left, there is a profile icon and the text 'Microsoft Team <no-reply\_msteam2@outlook.com>' and 'Windows Error Report'. On the right, it says 'Wed 8:54 AM'. The main body of the email is titled 'Windows User Alert' and 'Unusual sign-in activity'. The text describes a suspicious login attempt from a foreign IP address. A blue button at the bottom says 'Review recent activity'. Red circles highlight the sender information, the suspicious login attempt text, and the button.

Microsoft Team <no-reply\_msteam2@outlook.com> Windows Error Report

Wed 8:54 AM

Windows User Alert

## Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

**Sign-in details:**  
Country/region: Lagos, Nigeria  
IP Address: 293.09.101.9  
Date: 09/07/2016 02:16 AM (GMT)

If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately. 1-800-816-0380 or substitute you can also visit the Website: <https://www.microsoft.com/> and fill out the consumer complaint form. Once you call, please provide your **Reference no: AZ- 1190** in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

[Review recent activity](#)



service@intl.paypal.com <service.epaiypal@outlook.com>

log in

1/29/2016

Response required



## Response required.

Dear [\[redacted\]](#),

We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, [log in](#) to your account and go to the [Resolution Center](#).

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,  
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

Confirmation of your request from Hotels.com

MISC/Scams x



**Hotels.com** <Hotelscom@roktpowered.com>  
to dave

Nov 14, 2018, 11:38 AM (1 day ago)



[Hotels](#) [Hotel Deals](#) [Packages & Flights](#) [Groups](#) [Customer Service](#) [Gift Cards](#) [Secret Prices](#)



Hotels.com™

[New York Hotels](#)

[Las Vegas Hotels](#)

[Chicago Hotels](#)

[Los Angeles Hotels](#)

COUPON CODE

**\$50 off**

When you spend \$350 or more

EMLRKUSH21850:SK7CM6

[Book now](#)

**You must click through this email or book through our app to redeem this coupon.**

\*Use by 11:59 PM MT on 01/15/19 for travel by 04/30/19. Can't be used on some hotels. See details below.

**From:** Best Buy <BestBuyInfo@fashionlab.com.ua>  
**Subject:** Special Order Delivery Problem  
**Date:** ~~December 20, 2013 11:06:08 AM MST~~  
**To:** dave  
**Reply-To:** Best Buy <BestBuyInfo@fashionlab.com.ua>

[Hide](#)

My Best Buy ID: 002024460  
Reward certificate(s) available.



WEEKLY DEALS

GIFTS

[Tvs](#)

[Computers & Tablets](#)

[Cell Phones](#)

[Appliances](#)

[Cameras](#)

[Video Games](#)

[Audio](#)

Sir/Madam,

Your order [BBY-4983814314](#) has not been delivered because the specified address was not correct.  
Please fill this [form](#) and send it back with your reply to this message.

If we do not receive your reply within a week we will pay your money back less 17 because your order was reserved for the time of Christmas holidays.

Best Buy 7601 Penn Avenue South, Richfield, MN 49584-7655

BEST BUY, the BEST BUY logo, the tag design, [BESTBUY.COM](#), GEEK SQUAD, the GEEK SQUAD logo, MY BEST BUY, REWARD ZONE, BEST BUY MOBILE and the BEST BUY MOBILE logo are trademarks of BBY Solutions, Inc. All other trademarks or trade names are properties of their respective owners.





Thank you for your time today. If you have any questions please don't hesitate to call the LCIS Helpdesk at 419-213-4037 or email [lcishelpdesk@co.lucas.oh.us](mailto:lcishelpdesk@co.lucas.oh.us). Our staff will be happy to assist you with your questions or concerns.