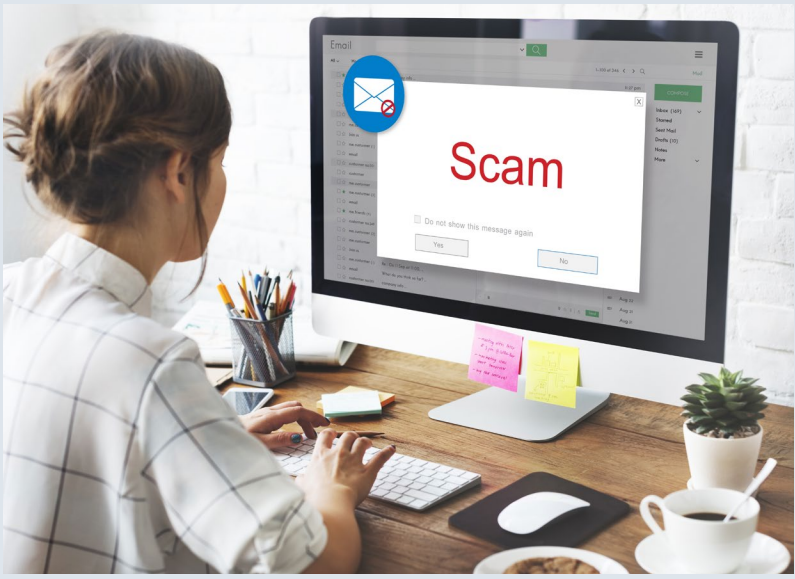
A Phishing Expedition:
How to Inform and Test Faculty Awareness of Email Scams

It happens all of the time. In fact, it might have happened to you this morning. An email appears in your Inbox. Or a text pops up on your phone. And it looks legitimate but just a little…off.

Well, you may have just been one of the thousands of people who, every day, are tricked by a phishing scam. In fact,according to the FBI, there were more than 26,000 victims of phishing scams reported in 2018.



A phishing scam is, in its most basic form, a means of obtaining sensitive information, such as passwords, bank account numbers, or Social Security numbers. If a "bad actor" gets access to this information, then they can do pretty much, well…anything and everything with it.

If you think you are immune from such attempts, think again. Cybercriminals are becoming more and more sophisticated in their attempts. They've come a long way since the classic Nigerian Prince scam (which still, apparently, rakes in some $700,000 a year). But, luckily, there are some "tells" that indicate that mysterious email or text may be less than sincere.

Signs of a Scam

- Firstly, these messages may appear as if they come from a familiar and trusted company. They often open under the guise of noting some suspicious activity regarding your account, and that you must confirm some personal information to rectify the situation. The reality is that the vast majority of legitimate companies won't ask you to provide sensitive information over email or text. Check the name of the person sending you the email by hovering over the "From" address. And be aware that some of these addresses may seem very close to being legitimate. But just think: why would a major company not own its own, proper domain?
- Here's an example of why all of those English classes you took in school may come in handy. Many scam email are rife with misspelling and poor grammar. Legitimate companies proofread their messaging to ensure a professional brand

experience. The content of scam emails is also often designed to make the reader panic, so that they react irrationally instead of thinking things through. Check the tone of the email to ensure that it is "professional".

- Usually phishing emails open with a generic greeting. But if you are a customer of a company that you routinely deal with, this company would call you by name and perhaps direct you to contact them by phone.
- Some emails are actually entirely hyperlinked (meaning, one large graphic where—no matter \ where you click—you are sent to a fake webpage, or harmful malware is downloaded to your device). This is a huge red flag as no reputable company would do this. Also, be sure to double check the true URL by rolling over it to ensure that it matches the URL displayed.
- Lastly, a scam email might also come with an attachment, masquerading as an invoice. Never, ever open an attachment unless you are expecting it. Period. Attachments and unknown links can install harmful malware. If an email or text asks you to click on a link or open an attachment, ask yourself if you have an account with the company. If no, it's a scam. If yes, reach out to the company through a website that you know is real, or by phone.

Hook, Line, and Sinker

It doesn't matter how powerful your firewall is or how advanced your security systems are. All it takes is one gullible employee reeled in by a phishing scam to put your whole network at risk.

In addition to education (such as sharing the tips above), another powerful way of measuring faculty scam knowledge is by literally putting it to the test.

A Phishing Test involves sending out a fake email and measuring the response. One approach could include setting up a bogus Gmail address and creating a form with Google Forms. If an employee receives the email then fills out the form, you will know and can either send the offending employees a gently castigating email or simply reward employees who didn't fall prey.

Sending phishing emails to your entire school or district at once might raise suspicion, so it's best to send them out over a specified time period.

To help with your efforts, here are several sample emails that you may customize to make them even more effective!

From: *Vendor [mail to: xxxxx]*
Sent: *[Date]*
Subject: *Your invoice is Available Now*

Hello _____,

Thank you for your business! It was a pleasure working with your district. Your bill for $572.63 was due [past date] however.

If you've already paid this invoice, then please ignore this email and sorry for troubling you. If you have not paid it, please do so as soon as possible to avoid incurring any penalties.

To view your invoice, visit: [URL]

If you have any questions regarding your invoice or would like to arrange alternate payment options, don't hesitate to get in touch.

Thank you,

Learning Systems Ltd.

[Download PDF]

From: *Google Education Fraud*
Sent: *[Date]*
Subject: *Someone is Using Your Password*

Hello [Name],

This email is to alert you to the fact that someone has just used your password to attempt signing into your Google Education account.

Incident Report:

[Date and Time]

Kyiv, Ukraine

Chrome browser

Google Education has stopped this sign-in attempt. We advise you to change your password immediately to avoid unauthorized access that could affect your school or district's systems.

Change Password [Link]

Sincerely,

The Google Education Fraud Team

From: *Data Safe Technologies*
Sent: *[Date]*
Subject: *Save Your Education Data Before It is Erased*

Hello [Name],

We have noticed that your school or district has not used your Data Safe account in quite a while. To better protect your student data, this account will be deleted in 14 days, so sign in now. [Link]

If you haven't experienced Data Safe services recently, they are worth another look. You do not want to risk the loss of your vital school operations and student data.

We hope to see you soon.

Sincerely,

The Data Safe Education Team

From: *ePayment*
Sent: *[Date]*
Subject: *Re: new payment on your account*

Hello [Name],

Please find attached the bank slip for the latest ePayment deposit in your account.

Regard,

ePayment Account Department

Link: [payment.zip]

From: *Branch Manager Kevin Wilson, USPS*
Sent: *[Date]*
Subject: *Canceled Delivery*

[Entire email is one large hyperlink so that if anyone clicks anywhere in the email, it will initiate a malicious attack]

[Graphic] Notification

Our courier couldn't successfully make the delivery of a parcel to you on [recent date]. Please print label and take it to your nearest post office before your parcel is returned. Thank you.

Print Shipping Label Now

[Footer] USPS. All rights reserved.

From: *Global Pay Network*
Sent: *[Date]*
Subject: *Restore Your Account*

Hello *[Name],*

We regret to inform you that your account has been restricted due to a potential security breach. To continue using your services, please download the file attached to this email and update your login information immediately.

© Global Pay Network Inc.

[Link that looks like document icon]

Follow Up with Finesse

After finishing your phishing campaign, follow up with an email to employees explaining why the emails were sent and what was learned. Use this as an opportunity to review various phishing attacks and how to spot them, and ask your staff to observe common email best practices such as not clicking on links or attachments from senders that they don't recognize and being watchful of email senders using suspicious domain names.

Above all, don't call out or embarrass any employee who may have fallen for your phishing scam. Hundreds of thousands of people are tricked by these types of attacks every day, and they are only growing in sophistication. Thank employees for doing their part to keep your school network, fellow staff, and—most importantly—students and their valuable data safe from these insidious cyberthreats.