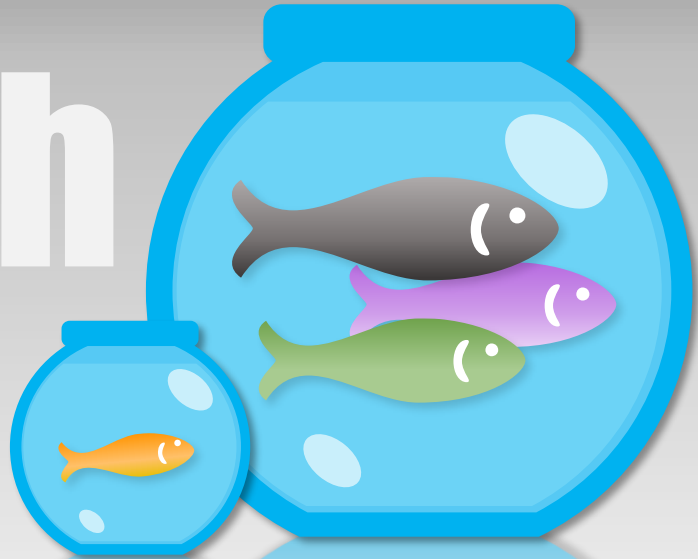


Phish Bowl



How not to be an easy target.....

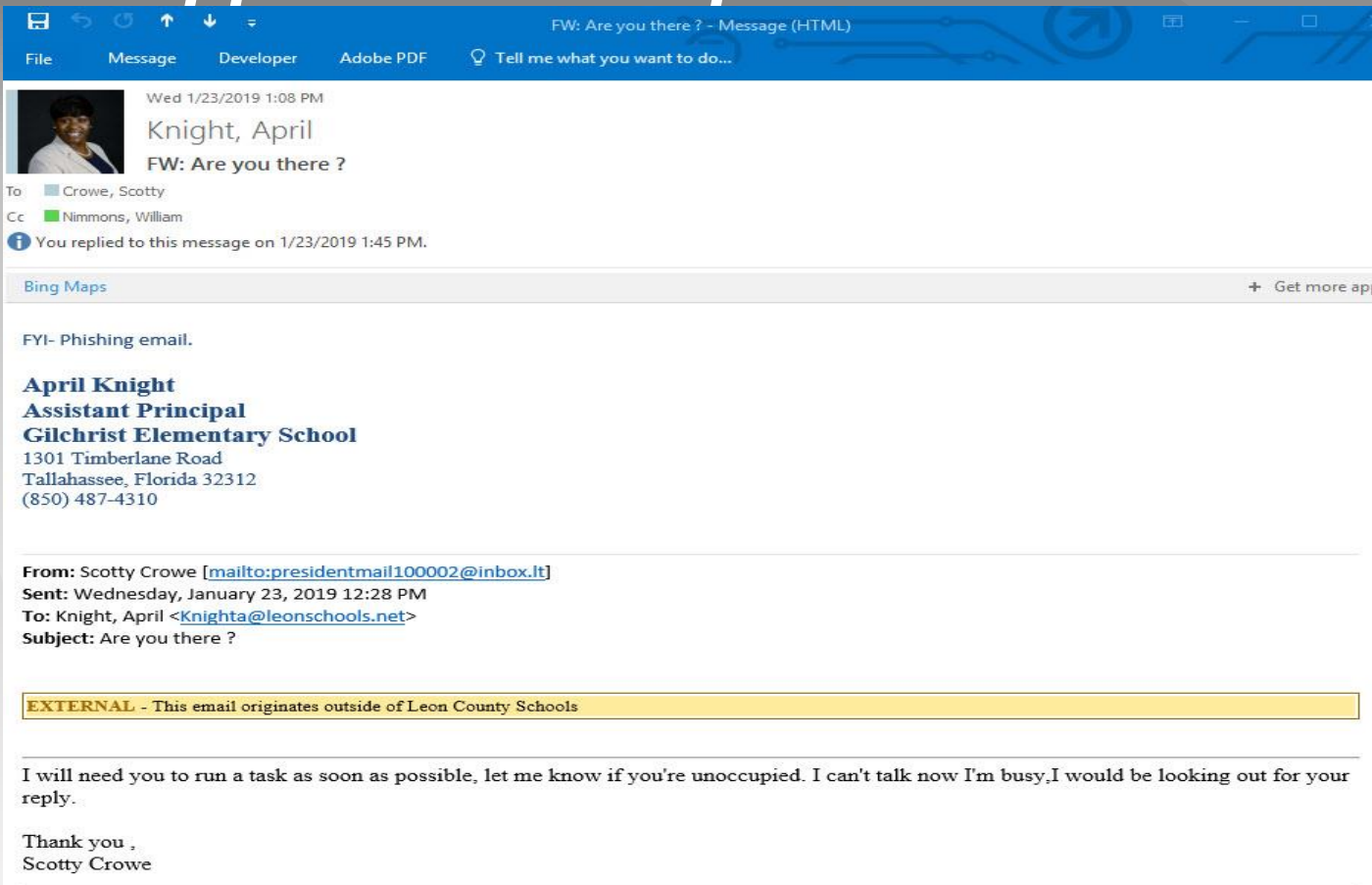
Phishing Attacks Target Everyone

Don't be the one
that gets caught!

I gave away my
credentials. HELP!!




It happens to Principals





The image shows a screenshot of an email client interface. At the top, there's a blue header bar with icons for file, message, developer, and Adobe PDF, along with a search bar. Below the header, the email content is displayed. It starts with a profile picture of a man and the subject line 'FW: Are you there ?'. The 'To' field lists 'Crowe, Scotty' and the 'Cc' field lists 'Nimmons, William'. A status bar indicates a reply on 1/23/2019 at 1:45 PM. The main body of the email is a phishing attempt from Scotty Crowe to April Knight, Assistant Principal at Gilchrist Elementary School. The email includes a yellow warning box stating it originates outside of Leon County Schools. The body text asks for a task to be run as soon as possible and ends with a thank you from Scotty Crowe.

Wed 1/23/2019 1:08 PM

Knight, April
FW: Are you there ?

To  Crowe, Scotty

Cc  Nimmons, William

 You replied to this message on 1/23/2019 1:45 PM.

[Bing Maps](#) + Get more apps

FYI- Phishing email.

April Knight
Assistant Principal
Gilchrist Elementary School
1301 Timberlane Road
Tallahassee, Florida 32312
(850) 487-4310

From: Scotty Crowe [<mailto:presidentmail100002@inbox.lt>]
Sent: Wednesday, January 23, 2019 12:28 PM
To: Knight, April <Knighta@leonschools.net>
Subject: Are you there ?

EXTERNAL - This email originates outside of Leon County Schools

I will need you to run a task as soon as possible, let me know if you're unoccupied. I can't talk now I'm busy,I would be looking out for your reply.

Thank you ,
Scotty Crowe

It happens to Assistant Principals

From: Erin Wheelis <mamzed@ssb-leipzig.de>

Date: Thursday, February 14, 2019 at 8:50 AM

To: David Rudenberg <rudenbergd@leonschools.net>

Subject: Transaction Refund 5886562652

EXTERNAL - This email originates outside of Leon County Schools

REFUND CONFIRMATION

Invoice Information

Description: Online Payment

Invoice Number 711889

Customer ID ES69789

[Open refund-receipt](#)

Total: 1306.00

Payment Information

Date: 02/05/2019

Transaction ID: 5886562652

Payment Method: Card ****7370

Transaction Type: Refund

Auth Code:

Merchant Contact Information

Erin Wheelis

erin.wheelis@fsu.edu

*SUNSHINE LAW AND PUBLIC RECORDS CAUTION: Florida has a very broad Public Records Law. Virtually all written communications to or from School Board of Leon County, Florida Personnel are public records available to the public and media upon request. E-mail sent or received on the LCSB system will be considered public and will only be withheld from disclosure if deemed confidential pursuant to State Law. Individual student records are

It happens to staff

From: AT&T <export@sunimpexcsa.com>

Date: January 28, 2019 at 3:32:38 PM EST

To: <KAILJ@leonschools.net>

Subject: AT&T payment update

EXTERNAL - This email originates outside of Leon County Schools

You added the following scheduled payment(s):

Service Type: Wireless

AT&T Account: 4324

Payment Method: BankDraft

Account Number: xxx802

Confirmation: 17B9ZE0OZEZA2D1

Payment Date: 01/28/2019

Amount: \$895.05

[View my bill](#)

Thanks for choosing us,
AT&T

It happens to IT staff



Mon 1/28/2019 8:27 AM

Evelo, Chris

FW: Your account has been hacked! You need to unlock.

To Nimmons, William; Dale Joiner; Fulton, Chris

You forwarded this message on 1/28/2019 8:29 AM.

Hello!

I have very bad news for you.

12/10/2018 - on this day I hacked your OS and got full access to your account eveloc@leonschools.net

So, you can change the password, yes... But my malware intercepts it every time.

How I made it:

In the software of the router, through which you went online, was a vulnerability.

I just hacked this router and placed my malicious code on it.

When you went online, my trojan was installed on the OS of your device.

After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts).

A month ago, I wanted to lock your device and ask for a not big amount of btc to unlock.

But I looked at the sites that you regularly visit, and I was shocked by what I saw!!!

I'm talk you about sites for adults.

I want to say - you are a BIG pervert. Your fantasy is shifted far away from the normal course!

And I got an idea....

I made a screenshot of the adult sites where you have fun (do you understand what it is about, huh?).

After that, I made a screenshot of your joys (using the camera of your device) and glued them together.

Turned out amazing! You are so spectacular!

I'm know that you would not like to show these screenshots to your friends, relatives or colleagues.

I think \$641 is a very, very small amount for my silence.

Besides, I have been spying on you for so long, having spent a lot of time!

Pay ONLY in Bitcoins!

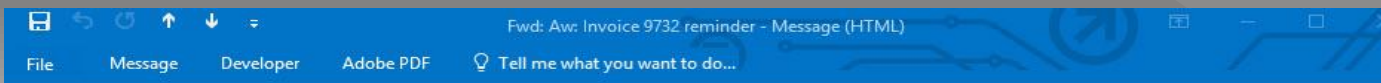
My BTC wallet: 145SmyE7DBEQExsnXZobojbQqr5UdgbCHh

You do not know how to use bitcoins?

Enter a query in any search engine: "how to replenish btc wallet".

It's extremely easy

It happens to School Board Members




Fri 1/25/2019 8:58 AM

Striplin, Alva

Fwd: Aw: Invoice 9732 reminder

To:  Nimmons, William

 You forwarded this message on 1/25/2019 11:04 AM.

Sent from my iPhone

Begin forwarded message:

From: Brown, Tina <purchasing@phil-union.com>

Date: January 25, 2019 at 8:56:03 AM EST

To: <striplina@leonschools.net>

Subject: Aw: Invoice 9732 reminder

EXTERNAL - This email originates outside of Leon County Schools

Please see attached and thanks!

[I have enclosed a copy of the invoice for your reference, you can download view using this link](#)

Brown, Tina

brownt4@leonschools.net

And...it happens to your teachers



Thu 1/31/2019 2:04 PM

Wagner, Brenda

FW: Are you available

To: Nimmons, William; Arango, Jimena

You replied to this message on 1/31/2019 4:14 PM.

Bing Maps

+ Get more apps

All of my teachers are getting this email. Not from me!!!

Mrs. Brenda Wagner, Principal
Killearn Lakes Elementary School
8037 Deerlake Drive East
Tallahassee, FL 32312
(850) 921-1265

A National Blue Ribbon School of Excellence



From: Barlowe, Lauren

Sent: Thursday, January 31, 2019 2:02 PM

To: Wagner, Brenda <wagnerb@leonschools.net>

Subject: Fwd: Are you available

Begin forwarded message:

From: Brenda Wagner <mailofprincipal50@gmail.com>

Date: January 31, 2019 at 1:55:46 PM EST

To: <barlowel@leonschools.net>

Subject: Are you available

EXTERNAL - This email originates outside of Leon County Schools

How are you doing now, Are you available right now ...

It happens to other school districts



WATCH LIVE NEWS WEATHER SPORTS ABOUT US CONTESTS

Hackers tried to steal \$2 million from Thomas County Schools' payroll



March 8, 2019 at 6:17 AM EST - Updated March 8 at 6:17 AM

THOMAS CO., GA (WCTV) - The Thomas County School System says a plot to hack into the district's payroll account has been foiled.

District officials say security protocols put in place by the district and its banking partner, TNB, prevented hackers from stealing nearly \$2 million from a school system account.

We're told the hackers obtained unauthorized computer files which contained accounting and payroll information and then tried to make fraudulent wire transfers to a series of out-of-state accounts.

District officials say even though the hackers were unable to get any money, they did gain access to payroll records. Those records include the names, employee identification numbers, bank account numbers, and bank routing numbers for school district employees.

It happens to city and county governments

USA TODAY

NEWS

SPORTS

LIFE

MONEY

TECH

TRAVEL

OPINION



81°

CROSSWORDS

MORE ▾



Cyberattack diverts almost \$500,000 out of city of Tallahassee payroll account

Karl Etters, Tallahassee Democrat

Published 9:50 p.m. ET April 5, 2019 | Updated 9:51 p.m. ET April 5, 2019



Critical settings so hackers can't access your bank account Kim Komando, for USA TODAY



CONNECT



TWEET



LINKEDIN



COMMENT



EMAIL



MORE

TALLAHASSEE, Fla. — Nearly half a million dollars was diverted out of the city of Tallahassee's employee payroll this week [after a suspected foreign cyberattack](#) of the city's human resources management application.

Hackers attempt every day to breach the city's security, officials say, but Wednesday's operation netted about \$498,000.

The employees have all been paid, said city spokeswoman Alison Faris, and officials are working to determine the hack's origins.

RingCentral



CLOUD PHONE



MEETINGS

With RingCentral
you get all in one
the fraction of time
of separate products

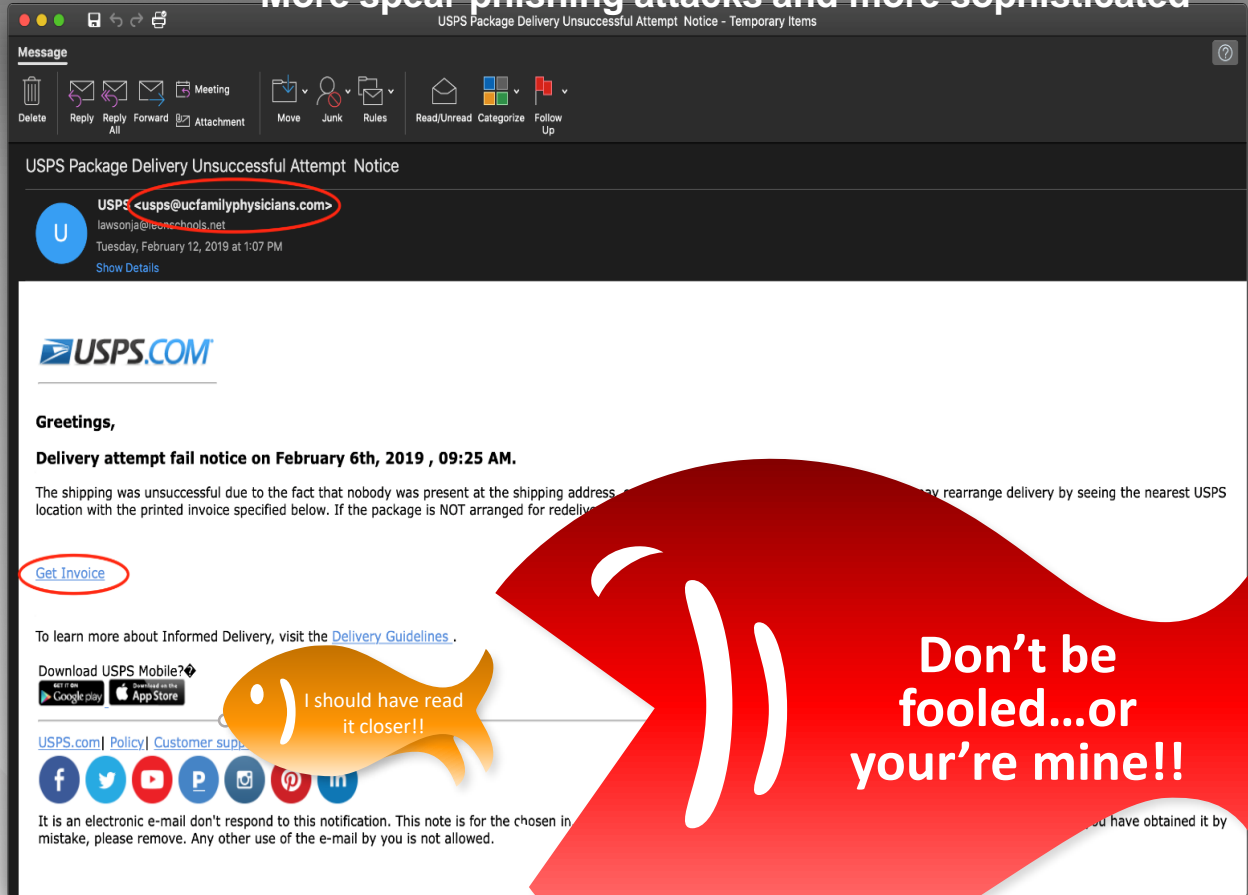
Get a quote

And...it happens to YOU!!



You can expect them to get worse

More spear phishing attacks and more sophisticated



Why you need Managed Phishing: Establish Your Baseline

Benchmark Phish-prone Percentage by Industry

Baseline Phish-prone Percentage (B-PPP)			
Industry	1 – 249 employees	250 – 999 employees	1000+ employees
Energy & Utilities	31.56	29.34	22.77
Financial Services	27.41	28.47	23.00
Business Services	29.80	31.01	19.40
Technology	30.68	30.67	28.92
Manufacturing	33.21	31.06	28.71
Government	29.32	25.12	20.84
Healthcare & Pharmaceuticals	29.80	27.85	25.60
Insurance	35.46	33.32	29.19
Not For Profit	32.63	25.94	30.97
Education	29.20	26.23	26.05
Retail & Wholesale	31.58	30.91	21.93
Other	30.41	28.90	22.85

Chart A

27%
**Avg. Initial
Baseline PPP**
across all industries and sizes

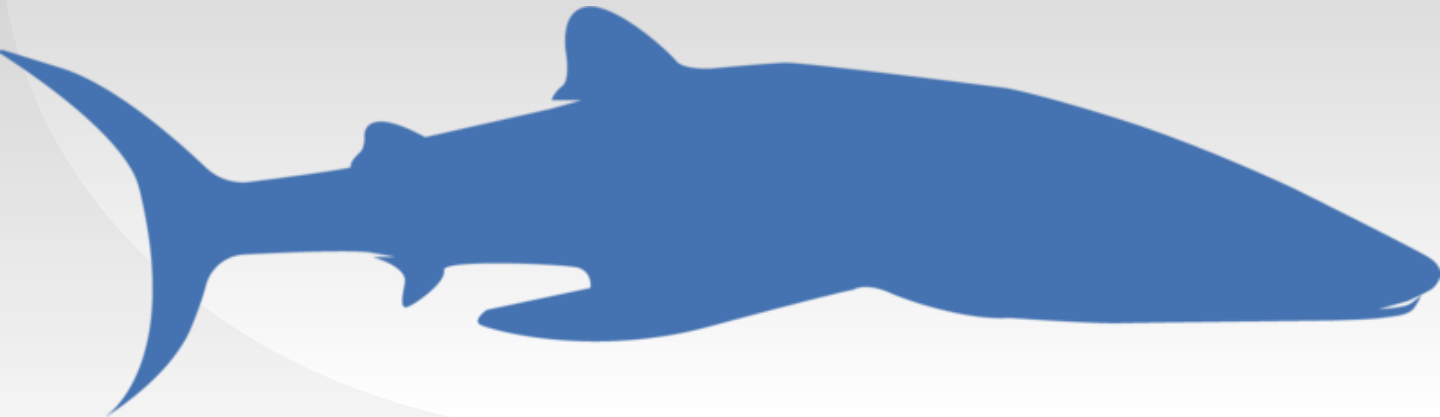
Average PPP by Size of
Organization

Org Size	Initial PPP
1 - 249	30.1 %
250 - 999	28.5 %
1000+	25.06 %

Don't be the one that gets caught!

Our LCS Baseline:

- 21% clicked the link
- 12% provided their userid/passwords
- 5,000 employees:
 - Clicked the link: 1,000
 - Provided credentials: 100



Why you need Managed Phishing: Drive the percentage down!!

Phase Three: After 12 Months of Combined Computer-based Training and Simulated Phishing Security Testing

At this stage, we measured only organizations that conducted 12 months of testing while adhering to best practice recommendations to run phishing tests at least once a month. The results were dramatic, showing that having a consistent, mature awareness training program took the average PPP from 27 percent all the way down to 2.17 percent – regardless of industry and size of organization. (Chart C)

Results after 12 Months of CBT and Phishing Testing

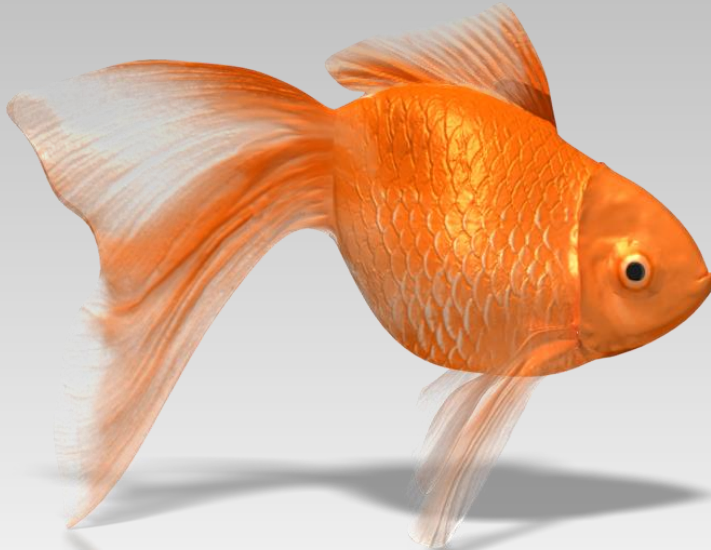
365 Day Phish-prone Percentage (365-PPP)			
Industry	1 – 249 employees	250 – 999 employees	1000+ employees
Energy & Utilities	2.83	1.87	5.56
Financial Services	1.54	2.22	5.81
Business Services	1.89	3.09	1.27
Technology	2.02	2.42	2.69
Manufacturing	2.16	3.13	2.47
Government	1.87	1.46	1.52
Healthcare & Pharmaceuticals	2.00	1.65	2.17
Insurance	2.23	2.68	5.26
Not For Profit	2.47	2.24	3.01
Education	2.80	1.91	5.31
Retail & Wholesale	2.14	1.87	2.68

2.17%
Avg.
One Year PPP
across all industries and sizes

Average PPP by Size of Organization

Org Size	12 Month PPP
1 - 249	1.94 %
250 - 999	2.21 %
1000+	2.04 %

Where we want it to be! 2-5%



Our solution for LCS:



- Priced for education!
- No limits on campaigns or number of users
- Effective and simple to use
- Easy to get started
 - Hosted solution



Demonstration Time!!
Charles Daffin