Cybersecurity – What Interesting Times…

Spring, 2018

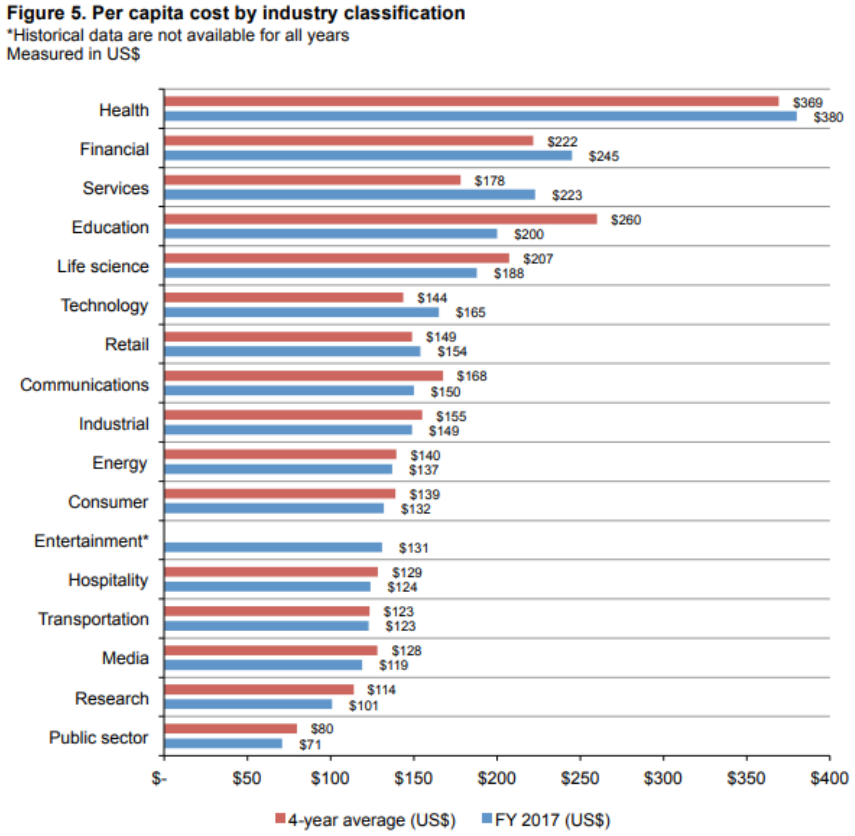
Teresa Macklin

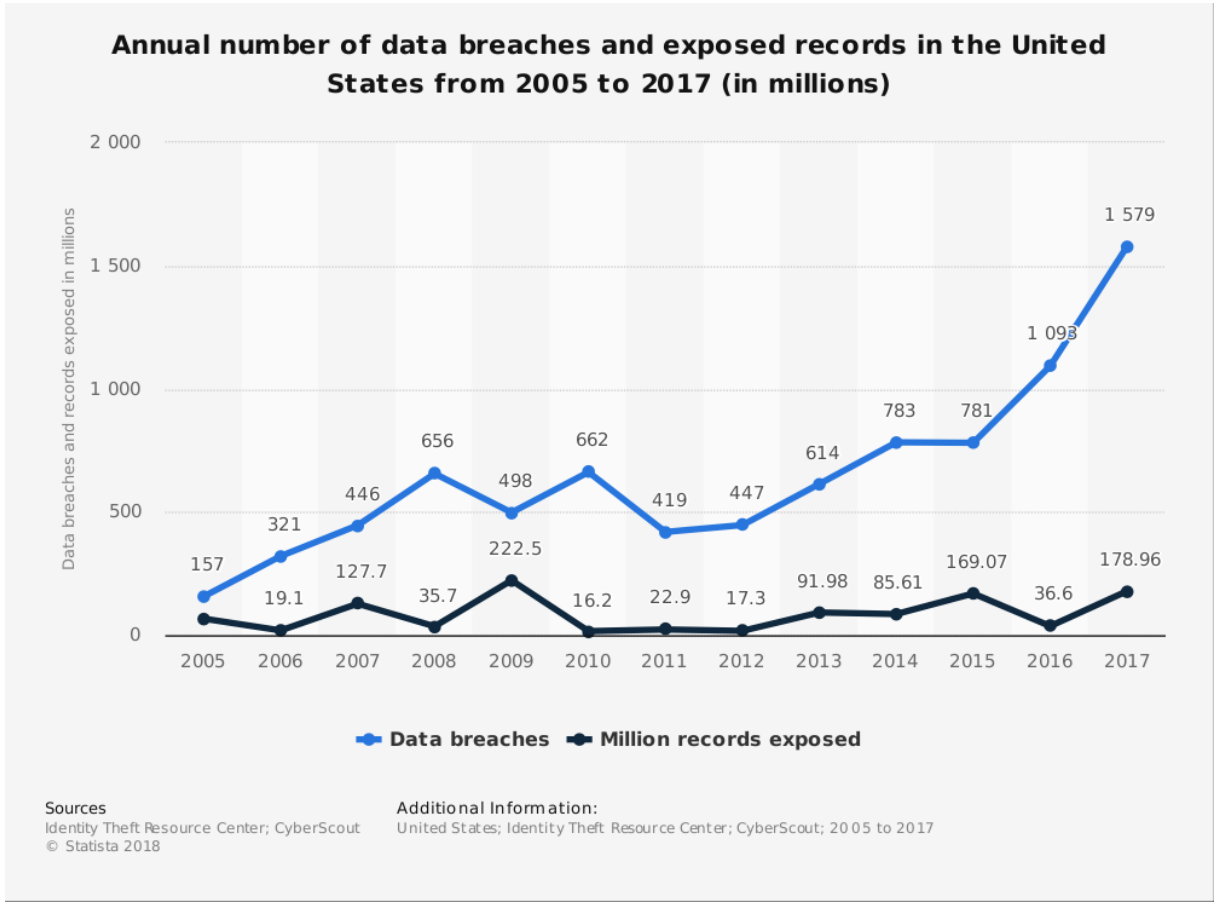
CSU San Marcos

Overview

- Current Environment
- What is the Problem We Are Trying to Solve?
- Current Threats & Patterns
- Advice for Personal Computers
- Advice for Small Business

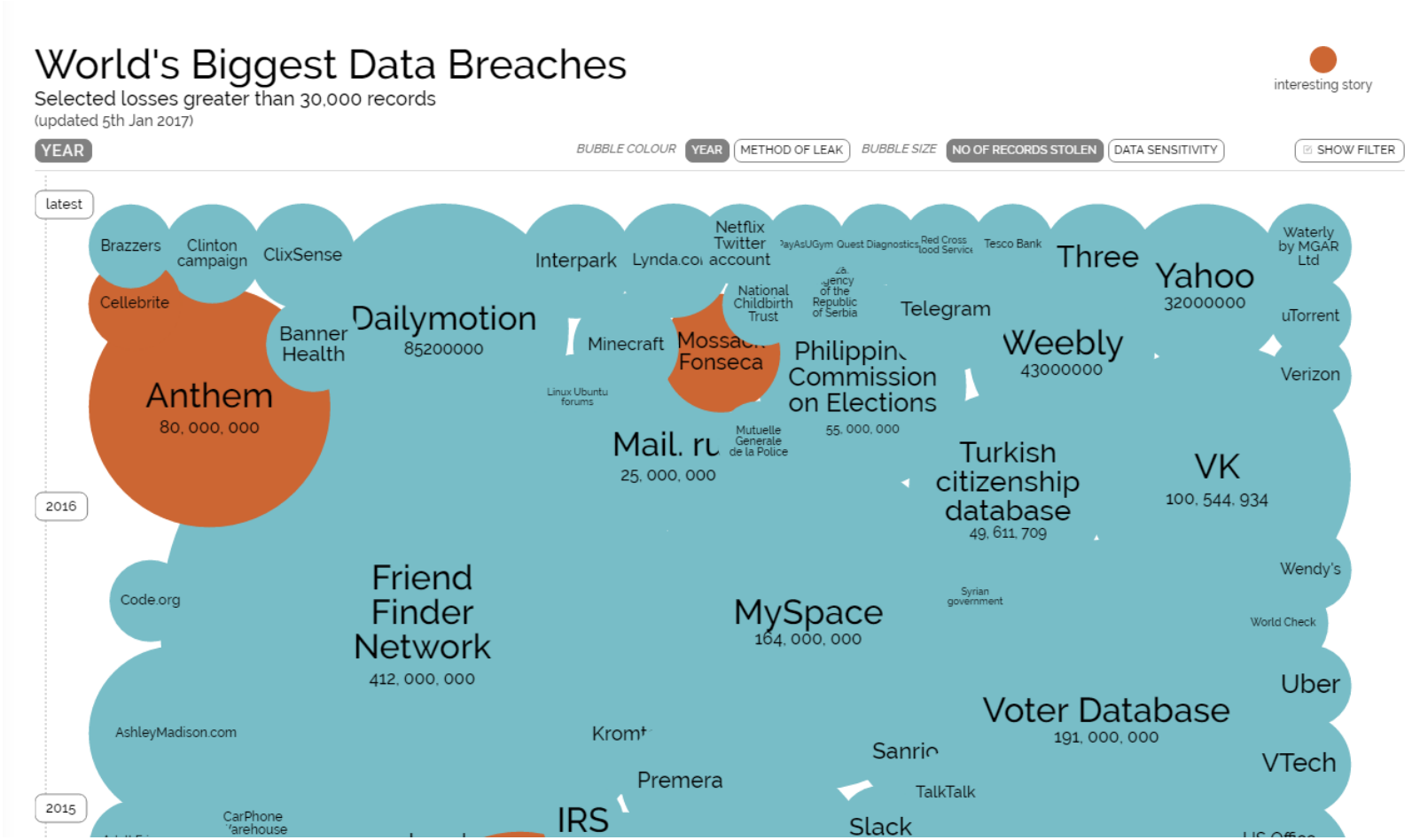
Upward Trends





From the Ponemon Report 2017: https://www.ibm.com/security/infographics/data-breach/

What does it look like?



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

INDUSTRY	POS INTRUS-ION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPION-AGE	EVERY-THING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48,49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

Threats Differ by Industry Sector

Why, Oh Why?

- Identity theft
- It is worth money!
- Fraud (healthcare, online transactions, payment card)
- Use of your computer resources
- Intellectual property theft
- Corporate espionage
- State espionage

Hacker service	Price
Social Security number (sold as part of 'Fullz' dossier)	$30
Date of birth	$11
Health insurance credentials	$20
Visa or MasterCard credentials	$4
American Express credentials	$7
Discover credit credentials	$8
Credit card with magnetic stripe or chip data	$12
Bank account number (balance of $70,000 to $150,000)	$300 or less
Full identity 'Kitz'	$1,200 to $1,300

The problem we are trying to solve

1. Only persons authorized to access information should get access to that information.
2. Both information and the systems used to access, store and manipulate it, should be available only to those persons authorized to alter the system or information and only under controlled circumstances.
3. The information (or systems) should be “intact” and not altered by intent or accident.

More recent: Devices! Control systems! Privacy! Not just information.

Threats!

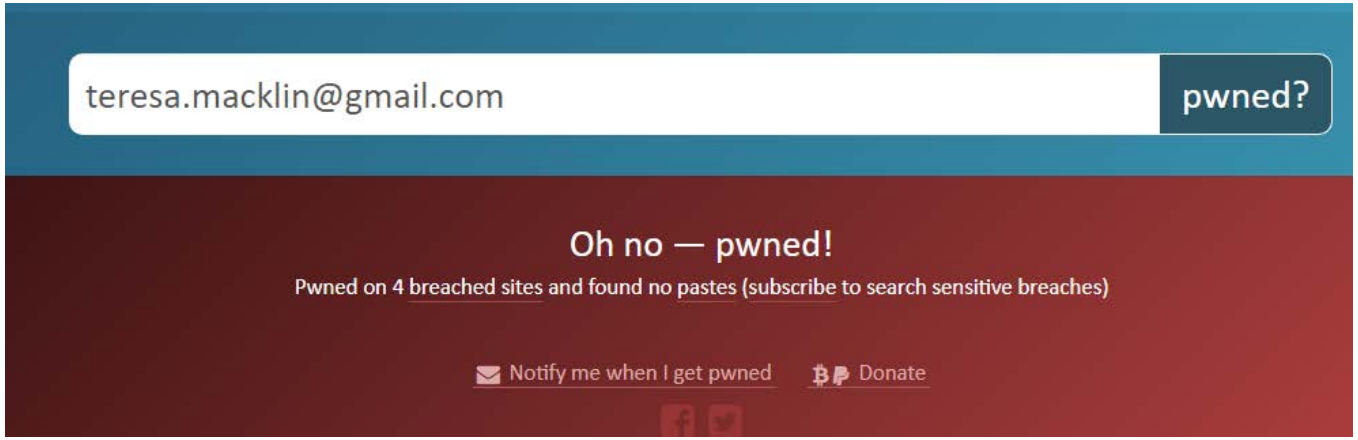
- Phishing (credentials)
- Fraud spear phishing (inducing you to pay)
- Malware (don’t click on that!)
- Ransomware
- Point of sale/payment card
- Insider threat

Phishing

- Phishing: Attempts to induce people to reveal confidential information.
  - Characteristics:
    - Urgent – “Your account will be deactivated!”
    - “Look-alike” – email will appear to come from a known sender. It will use their logo, graphics, etc.
    - Scam – the “Nigerian Prince” scenario
    - Threat – the “IRS Notice” or similar
    - Tech Support – “Your computer is infected!”

Phishing for Credentials – Why?

- With your username and password:
  - Access to current system
  - Will it work on google? Amazon? E-bay?
- Can your system be used for fraud?
  - Send millions of phishing messages from your account?
- https://haveibeenpwned.com/



Malware – Why?

- "Pwn" your computer systems to
  - Harvest your data
  - Make your computer part of a "botnet"
  - Use your computer to mine bitcoin
- Ransomware
  - May threaten to publish your data or
  - May encrypt your data and require you to pay to receive the encryption key

NEWS

Ransomware damage costs predicted to hit $11.5B by 2019

Cyber crime rises sharply amidst a decline in the percentage of victims willing to pay ransoms.



Phishing – Scam/Fraud

From: Richard Bernard <a1-rd20-7@btconnect.com>
Sent: Monday, March 5, 2018 9:25 PM
Subject: RV: SENT|[Tues| Mar, 06, 2018]

Write back for more details for this transaction.

I have sent you this message earlier, but your failure to respond has prompted me to re-sending it once again. It is about my late client who lost his life in an automobile accident along with his wife and only child.

I assisted him in making a deposit worth **$10.5M**. The Bank has therefore threatened to seize his account if an heir is not directly specified. You and my late client both share the same last name. With great respect, i want you to stand as an heir to the account so that his deposited funds can be released and transferred to you directly.

Kindly get back to my private email address for more update on this transaction (richrdbernard65@gmail.com)

Best Regards

Barrister Richard Bernard.



Wed 7/19/2017 10:00 AM
Kevin Morningstar <phoneoutlookmail@aol.com>
Re: Financials
To Barbara Sadnick
You replied to this message on 7/19/2017 10:00 AM.

It's vendor fees for advertising and consulting services. Amount value is $19,805.
I'll send the invoice and other documents later for internal reconciliation.
Should I forward the bank or check details so you can process the payment?
Sorry for the short notice, already promised the vendor that payment would be made soon.

Kevin Morningstar
Sent from mobile outlook...

-----Original Message-----
From: Barbara Sadnick <bsadnick@csusm.edu>
To: Kevin Morningstar <kmorningstar@csusm.edu>
Sent: Wed, Jul 19, 2017 9:52 am
Subject: RE: Financials

I can try.

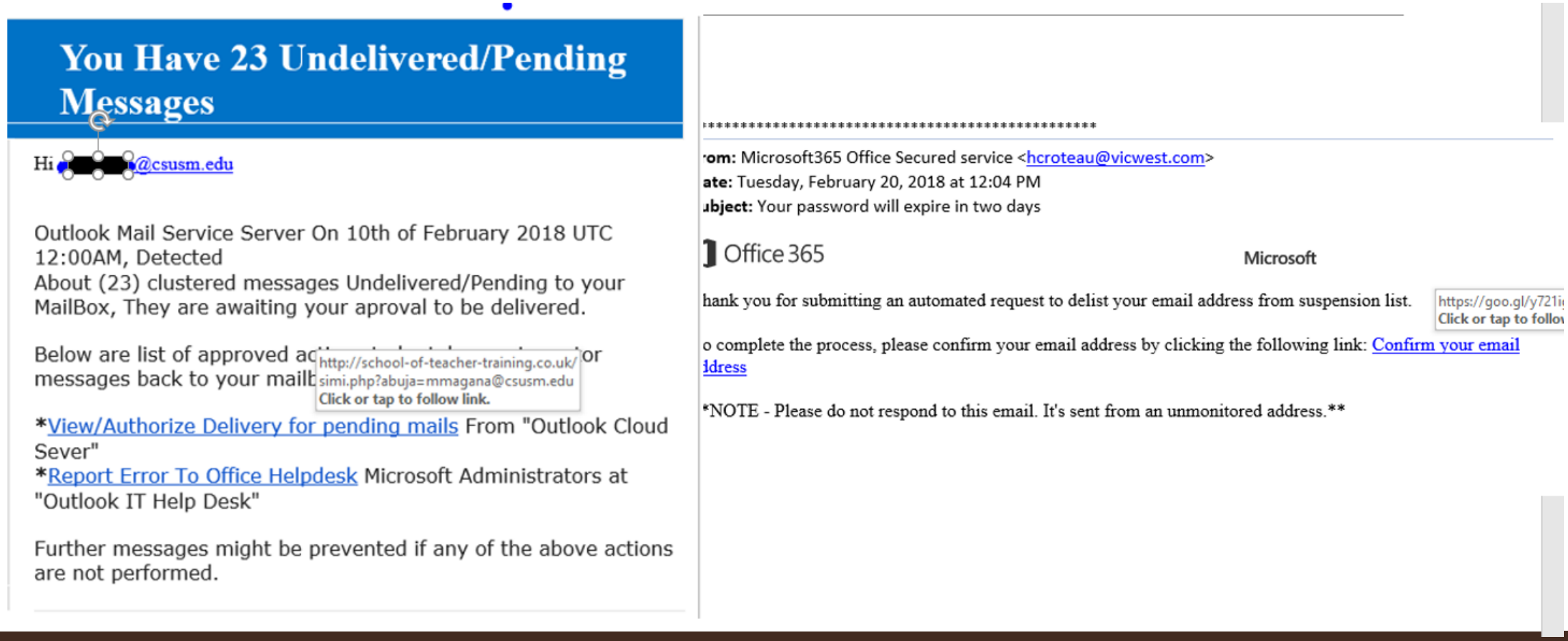
Barbara Sadnick
760-750-4771

From: Kevin Morningstar [mailto:kmorningstar@csusm.edu]
Sent: Wednesday, July 19, 2017 9:51 AM
To: Barbara Sadnick <bsadnick@csusm.edu>
Subject: Financials

There is an overdue payment that needs to be paid.
Let me know if you can sort so I can forward the details to you??

Regards
Kevin Morningstar
Sent from mobile outlook...

Phishing – Urgent Problem



You Have 23 Undelivered/Pending Messages

Hi [redacted]@csusm.edu

Outlook Mail Service Server On 10th of February 2018 UTC 12:00AM, Detected
About (23) clustered messages Undelivered/Pending to your MailBox, They are awaiting your aproval to be delivered.

Below are list of approved ac[illegible]or messages back to your mailb

http://school-of-teacher-training.co.uk/simi.php?abuja=mmagana@csusm.edu
Click or tap to follow link.

*View/Authorize Delivery for pending mails From "Outlook Cloud Sever"
*Report Error To Office Helpdesk Microsoft Administrators at "Outlook IT Help Desk"

Further messages might be prevented if any of the above actions are not performed.

****

om: Microsoft365 Office Secured service <hcroteau@vicwest.com>
ate: Tuesday, February 20, 2018 at 12:04 PM
ubject: Your password will expire in two days

Office 365 Microsoft

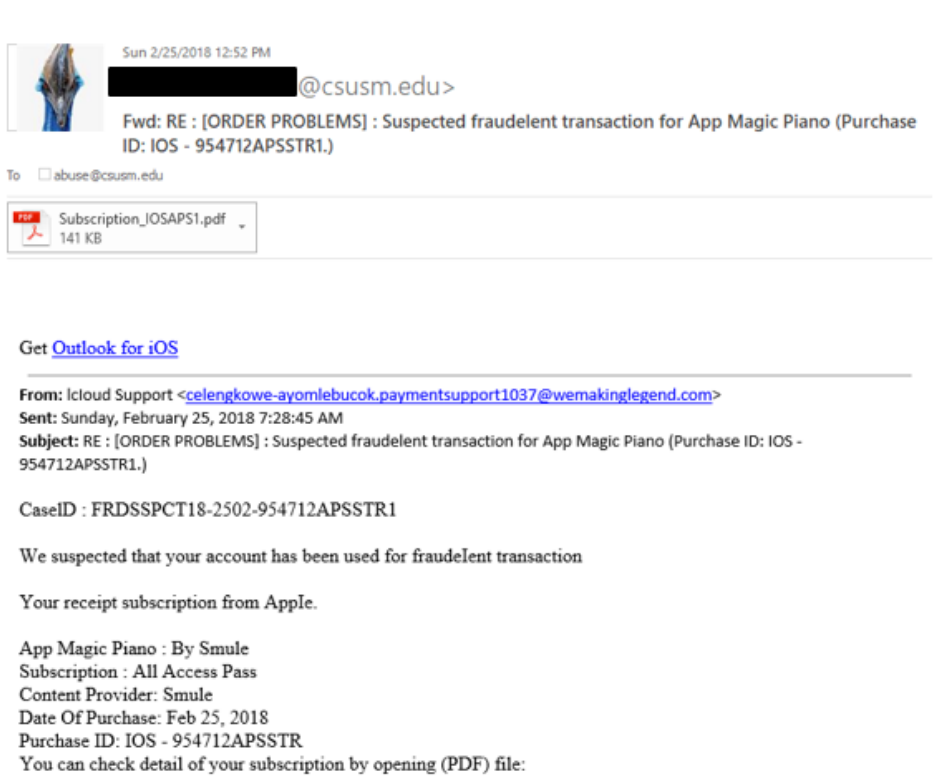
hank you for submitting an automated request to delist your email address from suspension list.

https://goo.gl/y721i
Click or tap to follo

o complete the process, please confirm your email address by clicking the following link: Confirm your email ddress

*NOTE - Please do not respond to this email. It's sent from an unmonitored address.**

Malware by Email



Sun 2/25/2018 12:52 PM

[redacted]@csusm.edu>

Fwd: RE : [ORDER PROBLEMS] : Suspected fraudelent transaction for App Magic Piano (Purchase ID: IOS - 954712APSSTR1.)

To abuse@csusm.edu

Subscription_IOSAPS1.pdf
141 KB

Get Outlook for iOS

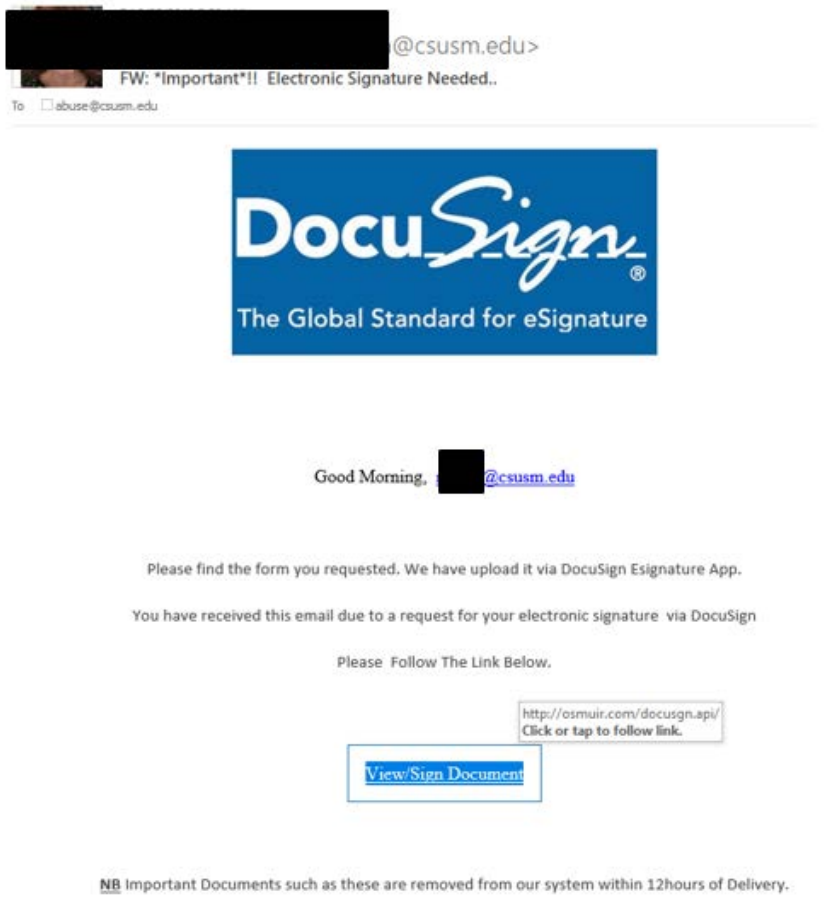
From: Icloud Support <celengkowe-ayomlebucok.paymentsupport1037@wemakinglegend.com>
Sent: Sunday, February 25, 2018 7:28:45 AM
Subject: RE : [ORDER PROBLEMS] : Suspected fraudelent transaction for App Magic Piano (Purchase ID: IOS - 954712APSSTR1.)

CaseID : FRDSSPCT18-2502-954712APSSTR1

We suspected that your account has been used for fraudelent transaction

Your receipt subscription from Apple.

App Magic Piano : By Smule
Subscription : All Access Pass
Content Provider: Smule
Date Of Purchase: Feb 25, 2018
Purchase ID: IOS - 954712APSSTR
You can check detail of your subscription by opening (PDF) file:



[redacted]@csusm.edu>

FW: *Important*!! Electronic Signature Needed..

To abuse@csusm.edu

DocuSign
The Global Standard for eSignature

Good Morning, [redacted]@csusm.edu

Please find the form you requested. We have upload it via DocuSign Esignature App.

You have received this email due to a request for your electronic signature via DocuSign

Please Follow The Link Below.

http://osmuir.com/docusgn.api/
Click or tap to follow link.

View/Sign Document

NB Important Documents such as these are removed from our system within 12hours of Delivery.

How we solve the problem

- Policy – organizational rules for managing security
- Process – secure operations and practices, patching, identity, backups…
- Products – secure applications, thoughtful use of features
- People – awareness, acceptance, training

For the Personal Computer

- Install and maintain an anti-virus program
- Install every security update – java, adobe, operating system… all of them. Every time.
- Look for and avoid those phishing messages (and phone calls!)
- Use a unique password everywhere
  - Use a password manager program
- Enable multi-factor authentication everywhere
- Be careful about connecting to unknown wireless networks

For the Small Business

- All of the previous slide PLUS
- Pay attention to the C I A (confidentiality, integrity, availability)
- Create a security program –
  - https://www.fcc.gov/general/cybersecurity-small-business
  - https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
- Ensure that your employee accounts are current (do you promptly remove exited employees?)
- Train your people! Many cybersecurity breaches are caused by errors.
- Do a risk assessment!
- Encrypt your confidential data!
- Recognize that security is necessary, and sometimes not convenient