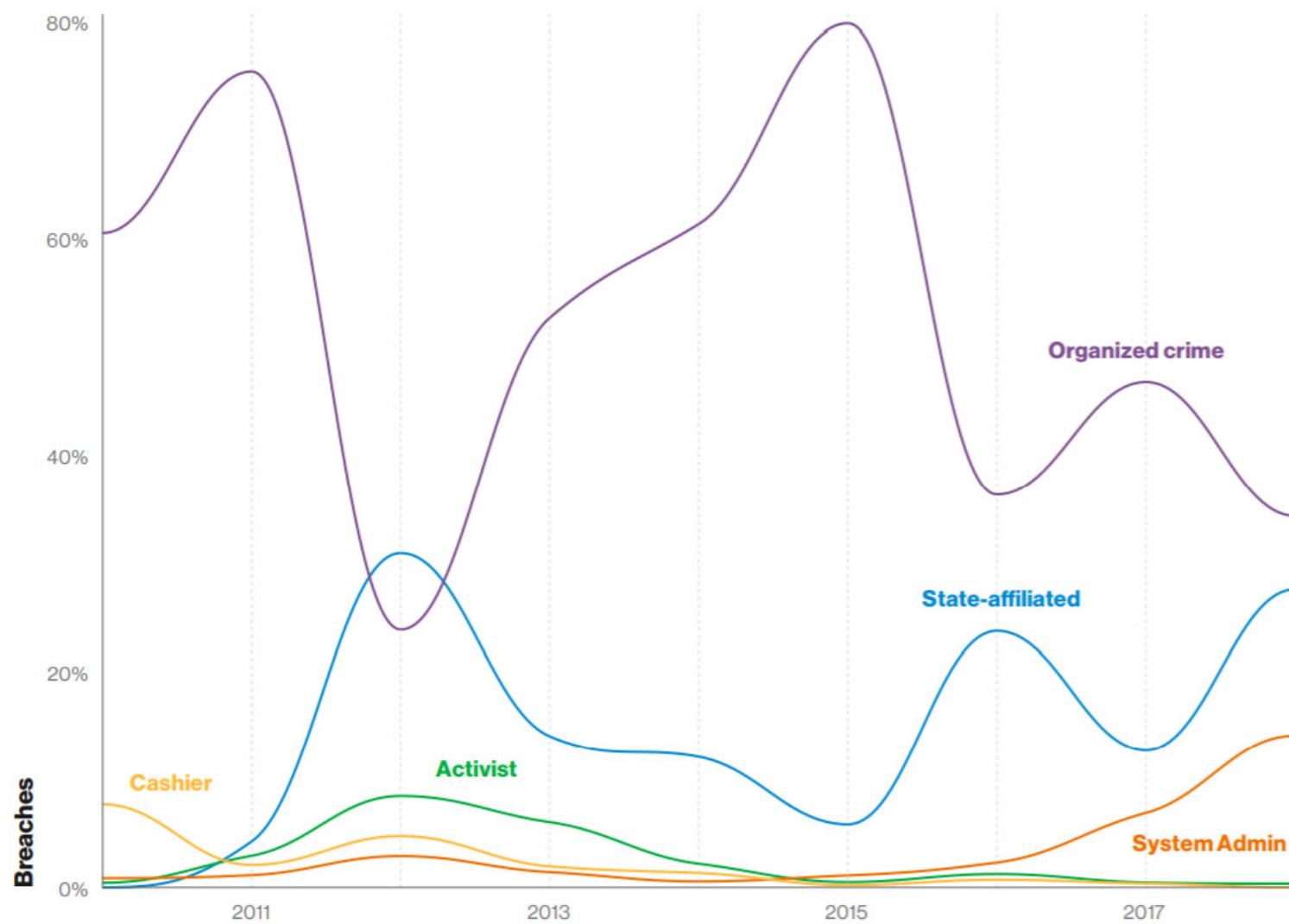


# ~~Pwned~~: Protecting Yourself in the 2019

By Dallin Warne

# Why are you a target?

- 99% Money
- 1% Everything else (revenge, activism, hate, espionage, etc)
- Why do they do it?
  - Because it works.
  - 3%-5% clicks on phishing links, down from 25% in 2012



**Figure 8.** Select threat actors in breaches over time

## By the Numbers

- 52% of breaches involved hacking
  - 32% of breaches involved phishing
  - 28% of breaches involved malware
- 
- (Numbers don't add up to 100% because of overlapping techniques)

# Ways to Protect Yourself

- Musts
  - Keep everything updated—Computer, phone, webcam, router, oven, etc.
  - Antivirus (Windows/Mac/Phone)
  - Multi-factor authentication
  - Password manager (Lastpass, 1Password, etc)
  - Ad-blocker
  - Haveibeenpwned notifications
  - Use credit cards for online purchases and only on reputable sites
  - Screen calls from unknown numbers
    - Hiya, Android scam alert
- What to watch out for
  - Social media scams
  - Being sent to unsolicited offers
  - Outdated-looking or broken websites
  - Browser security warnings
- Shoulds
  - Credit Monitoring (Free through bank/bureau)
  - Freeze your credit at Big 3
  - Bank and card transaction notifications
  - Check for card skimmers

# Obvious Signs



**Sender's email is from  
an unofficial domain or  
unknown number**



**Generalized**

Dear  
Customer/sir/madam/anything  
but your name



**Poor English**

Bad grammar or spelling  
Abnormal conversational words

# Common Phishing Signs

- Unexpected
- Act urgently
- Negative or positive consequences for inaction/action
- Piques curiosity
- Must take an action within the email. Unavailable to verify outside of it.
- Money in any form including gift cards, rebates, sales, etc
- Links
  - Website name is weird, or similar but not quite to what is expected.
  - URL shorteners
  - Lots of % in the [link](#)  
(%3Cscript%3Ealert(%27I%20got%20you.%27)%3B%3C%2Fscript%3E)
- Attachments—especially documents and compressed files

# Advanced—Spear Phishing

- Uses *Social Engineering*
- Personal
- Can include details about you, a customer or supervisor, etc
- Relevant to you
- Based on information that's publicly available
- Enticing
- Known contacts' accounts hacked



# What to do

- Stop and think it through.
- Be paranoid.
- Verify by other means, *especially when sending money or given a login page*
  - Go directly to the website yourself without clicking on anything in the message
- Sometimes you can just wait.

# Example: Sent to a Librarian

RE: I shared PDF with you in OneDrive

✕ DELETE   ← REPLY   ⇐ REPLY ALL   → FORWARD   ⋮

Mark as unread



Library Publishing Coalition (LPC) <mjkktwo@aol.com>

2018 12:44 PM

📎 1 attachment

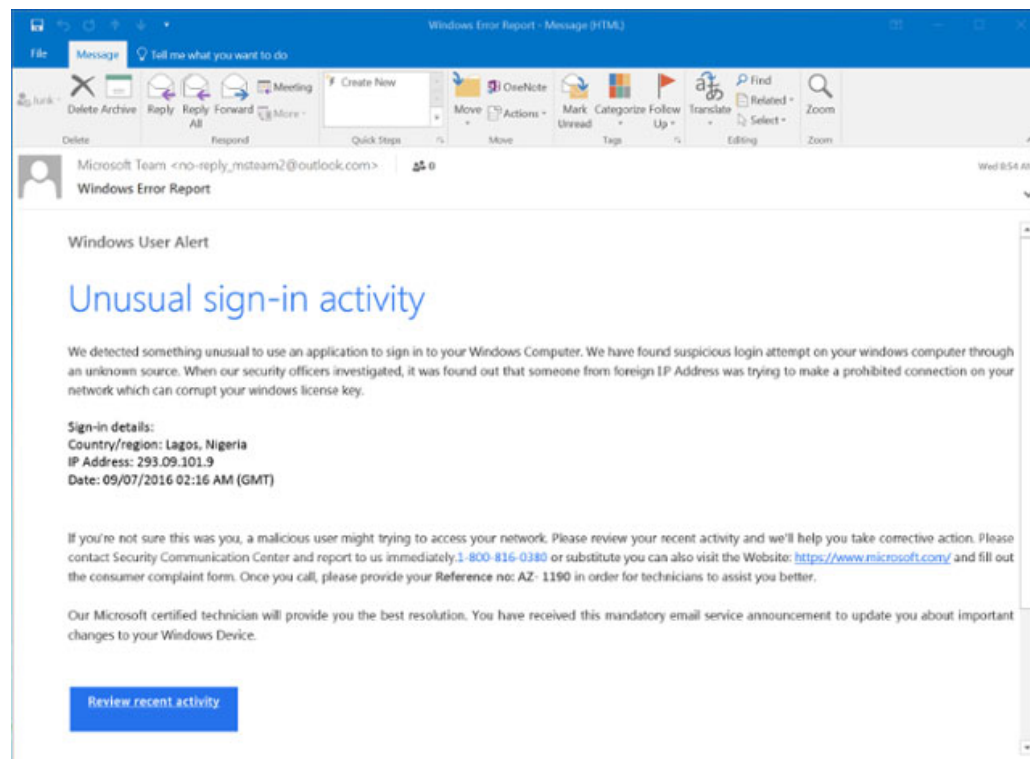


I have sent A secure document to you using OneDrive.  
Go ahead and click the PDF attached to view your document,  
This entails a project information,I want you to verify and send me your own ideas on how we can make it a success.

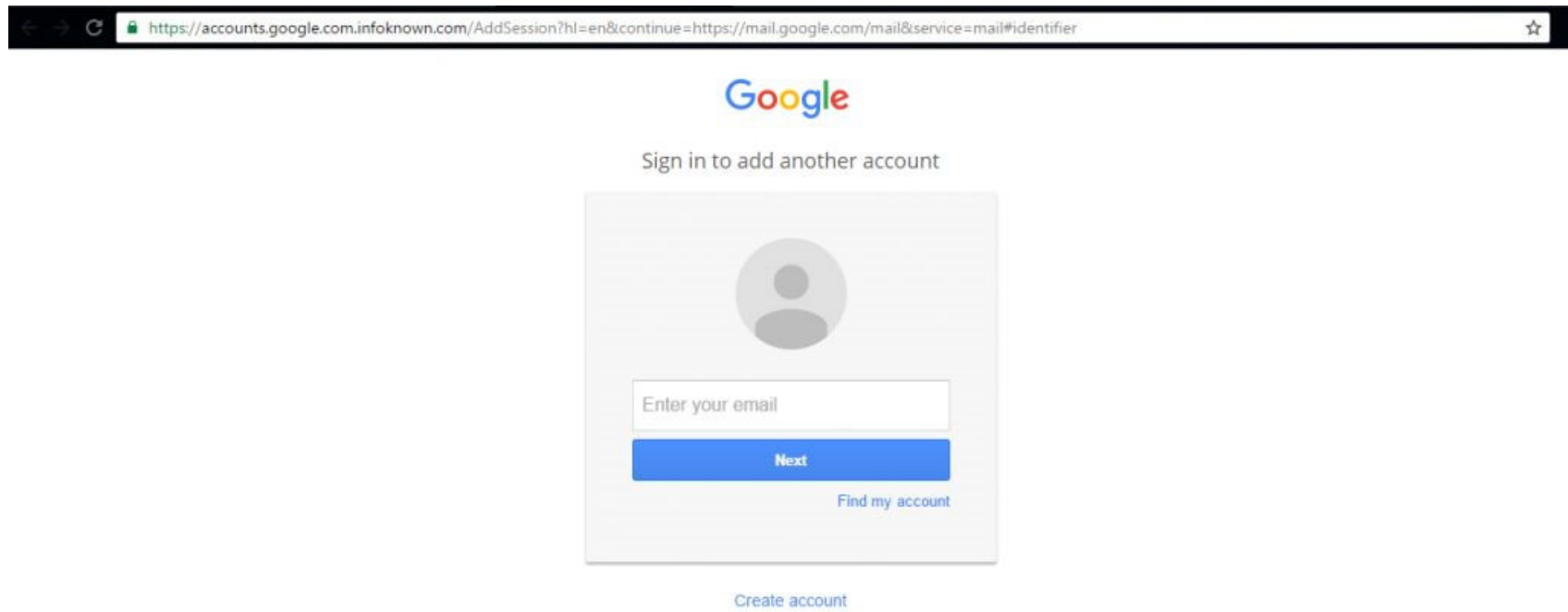
Regards,

Dr. Katherine Skinner  
Executive Director  
1230 PEACHTREE STREET, SUITE 1900  
ATLANTA, GA 30309

## Example 2



# Example 3



A screenshot of a web browser displaying a Google account sign-in page. The browser's address bar shows the URL: `https://accounts.google.com/infoknown.com/AddSession?hl=en&continue=https://mail.google.com/mail&service=mail#identifier`. The page features the Google logo at the top, followed by the text "Sign in to add another account". Below this is a light gray box containing a circular profile icon placeholder, a text input field with the placeholder text "Enter your email", a blue "Next" button, and a link "Find my account". At the bottom of the page, there is a link "Create account".

Google

Sign in to add another account

Enter your email

Next

Find my account

Create account

## Example 4

**VANGUARD BROKERAGE SERVICES** <id@proxyvote.com>  
Reply-To: VANGUARD BROKERAGE SERVICES <ProxyMaster@proxyvote.com>  
To: [REDACTED]

Fri, Mar 2, 2018 at 2:53 A



### A message from Vanguard Brokerage Services®

Dear Vanguard client,

You elected to receive shareholder communications electronically via the Internet.

This is a notification that **VANGUARD FUNDS** has released important information to its shareholders. You can view this information at the following Internet website:

Shareholder Letter

[https://materials.proxyvote.com/Approved/MC0151/20180223/SHLTR\\_347518.PDF](https://materials.proxyvote.com/Approved/MC0151/20180223/SHLTR_347518.PDF)

#### Contact us

If you have any questions, please call Vanguard Brokerage Services at **800-284-7245** on business days from 8 a.m. to 10 p.m., Eastern time.

#### Legal notices and e-mail administration

If you elected e-delivery of account documents at [vanguard.com](http://vanguard.com) and want to change your election to U.S. mail, log on to [vanguard.com](http://vanguard.com) and update your mailing preferences. Please don't reply to this message to opt out.

# Example 5



This is an automated email, please do not reply

## Zelle Pay Payment Transfer

Dear Member,

A new payment was sent to your USAA account using ZellePay Transfer. To accept the payment, You are immediately required to validate your account.

[VALIDATE YOUR ACCOUNT](#)

Payment will be posted into your account within 24 hours after validation.

Regards,  
USAA - ZellePay



© All users of our online services subject to Privacy Statement and agree to be bound by Terms of Service. Please review. © 2018 USAA. All rights reserved.

# Example: Extortion

**From:** Rodie Kaustinen <fcerwinzux@outlook.com>  
**To:** [REDACTED]@[REDACTED]  
**Subject:** Name, Password  
**Date:** [REDACTED] 2018 21:22:07 +0000

I know [REDACTED] is your pass. Lets get directly to point. None has compensated me to investigate you. You don't know me and you're most likely wondering why you're getting this mail?

In fact, I setup a malware on the X vids (pornographic material) site and guess what, you visited this website to have fun (you know what I mean). While you were watching video clips, your web browser initiated functioning as a Remote Desktop having a key logger which provided me with accessibility to your display screen as well as cam. Just after that, my software collected all of your contacts from your Messenger, FB, as well as emailaccount. And then I created a video. 1st part displays the video you were viewing (you have a nice taste : )), and second part displays the view of your cam, and it is you.

You have two possibilities. Shall we study these types of solutions in aspects:

1st alternative is to dismiss this email. In this instance, I most certainly will send out your actual video to every bit of your personal contacts and thus you can easily imagine about the embarrassment you experience. Do not forget if you happen to be in a romance, just how it is going to affect?

In the second place solution should be to give me \$7000. Let us think of it as a donation. In this scenario, I will straightaway erase your videotape. You will keep your way of life like this never happened and you will never hear back again from me.

You will make the payment through Bitcoin (if you don't know this, search for "how to buy bitcoin" in Google).

BTC Address to send to: 1Cu3Fp2Rgpknfv9avHePD5H448YVoanLgQ  
[case sensitive copy and paste it]

If you are wondering about going to the cop, very well, this email message can not be traced back to me. I have taken care of my moves. I am just not trying to charge a fee much, I just like to be rewarded. I have a specific pixel in this email message, and at this moment I know that you have read this email. You now have one day in order to make the payment. If I don't get the BitCoins, I will definitely send out your video to all of your contacts including relatives, coworkers, and many others. Nonetheless, if I do get paid, I will destroy the video right away. If you want evidence, reply with Yup & I definitely will send your video recording to your 10 contacts. It is a non:negotiable offer that being said do not waste my time and yours by replying to this e mail.

# Payback

- [https://www.ted.com/talks/james veitch this is what happens when you reply to spam email#t-108537](https://www.ted.com/talks/james_veitch_this_is_what_happens_when_you_reply_to_spam_email#t-108537)



# The 773 Million Record "Collection #1" Data Breach



17 JANUARY 2019

## Billing Details for 11.9M Quest Diagnostics Clients Exposed

By [Sergiu Gatlan](#)

 June 3, 2019  09:41 AM

# Equifax's massive 2017 data breach keeps getting worse

# Password

- Two biggest ways to reduce risk:
  - *Long, unique* password from a password generator
    - Complexity matters less
  - Multi-factor authentication

# Multi-factor authentication

- Best method is hardware-based, push notifications, or time-based codes
- Text messages or emails aren't as secure, but significantly better than passwords alone
- Duo, Google, Microsoft all produce decent apps

# Passwords are so 1990s

- PassPhrase or PassSentence, not password
- [16+ characters.](#)
- 6 words from 2000 words = 63,521,358,201,095,760,000 possible combinations.
- *WizzoWazzo is Hilarious, Girls can't eat 14 pizzas*
- Passwords are like tissues: Don't reuse them. Have unique passwords as much as possible.
- Use a password manager (Lastpass, 1Password, etc)
- Don't use passwords that are already hacked
- Check out <https://haveibeenpwned.com>

# Password Managers

- LastPass—Free, cloud-based.
  - Adequate for most consumers
- 1Password—\$36/year, cloud-based
- Other free/paid available

# Utah Security Breach Law

- “If an investigation under Subsection (1)(a) reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident.
- <https://le.utah.gov/xcode/Title13/Chapter44/13-44-S202.html>
- Weak consumer protection

## **Is it a Phish?**

- Is the sender's email address correct?
- Is it an unsolicited email?
- Does it give a sense of urgency?
- Does it ask for money or to buy something?
- Is there a document attached?
- Does it ask you to log in or give personal info?
- Can you verify the request outside the email?
- Hover over the links:
  - Do they take you to a known website? Or does it look strange?
  - Are there a lot of % symbols?