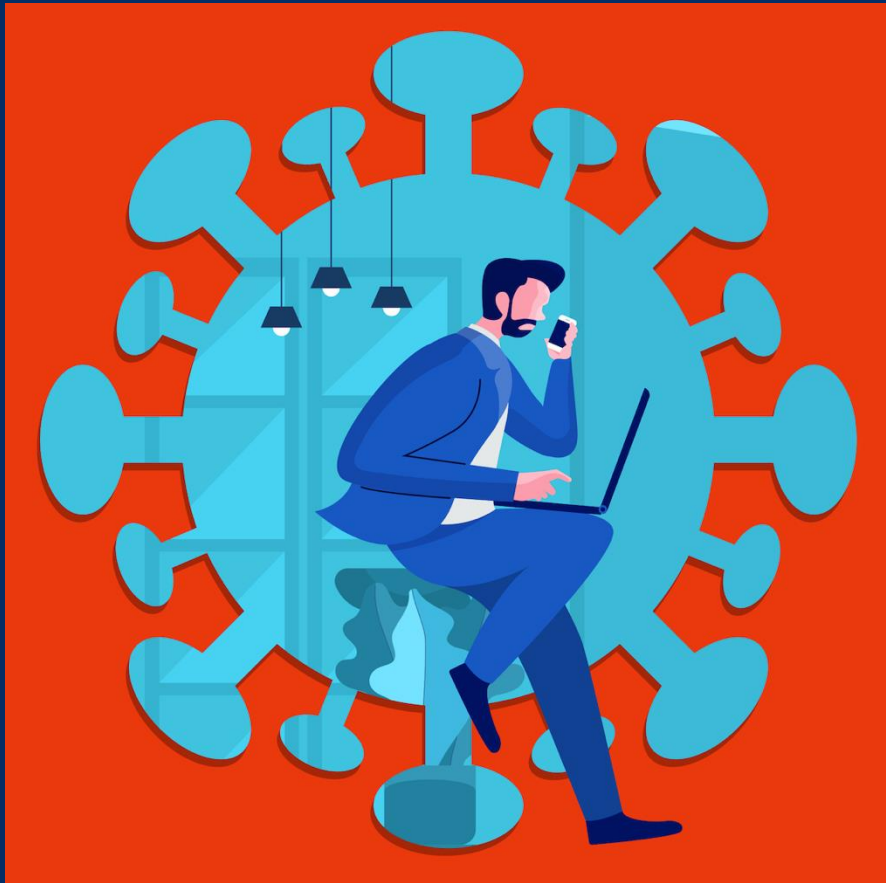


# Remote Work Security

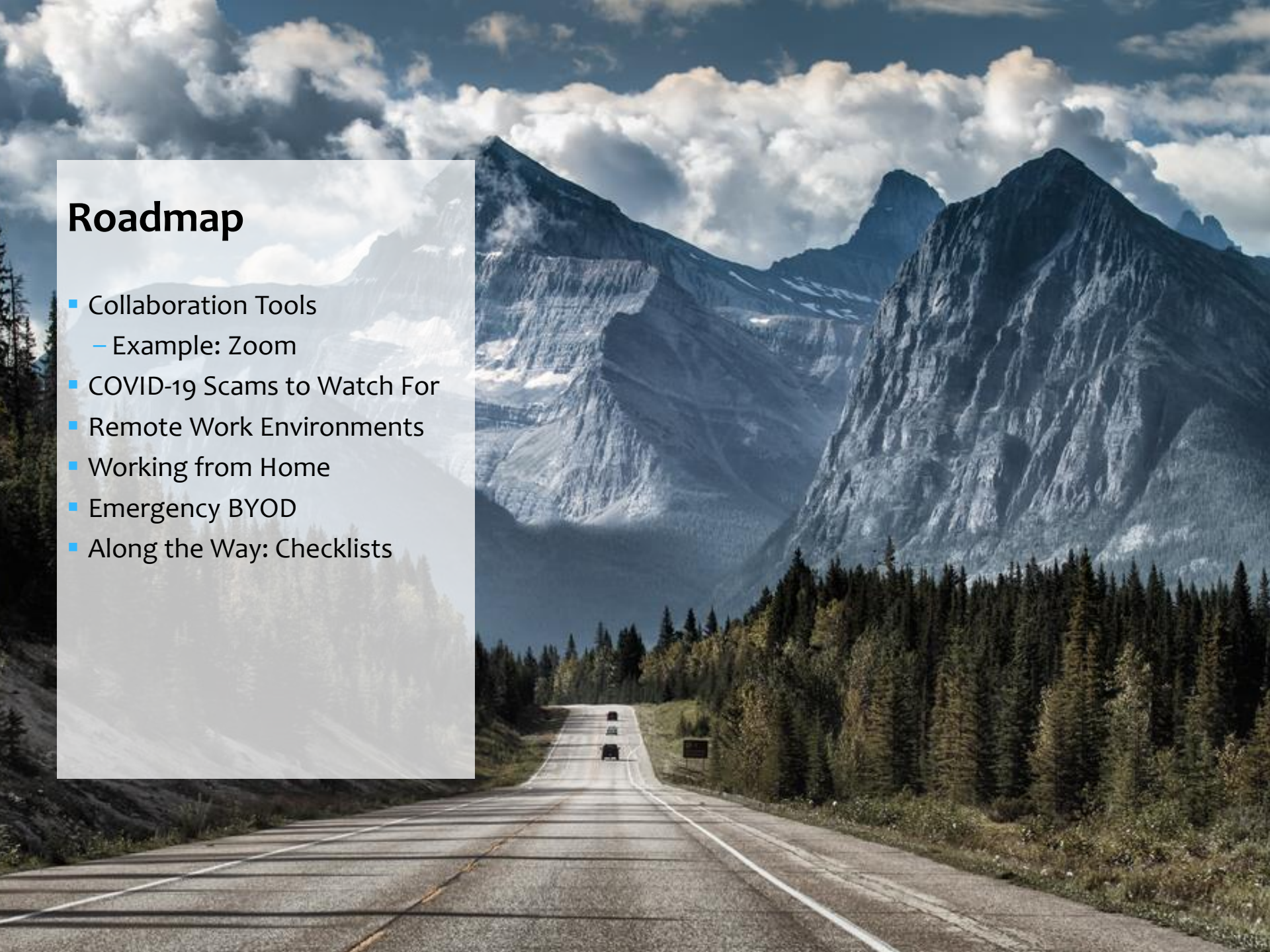


Sherri Davidoff  
CEO



# Roadmap

- Collaboration Tools
  - Example: Zoom
- COVID-19 Scams to Watch For
- Remote Work Environments
- Working from Home
- Emergency BYOD
- Along the Way: Checklists



# Over 500,000 Zoom accounts sold on hacker forums, the dark web

By Lawrence Abrams

April 13, 2020

02:05 PM

6



Password

Host PIN

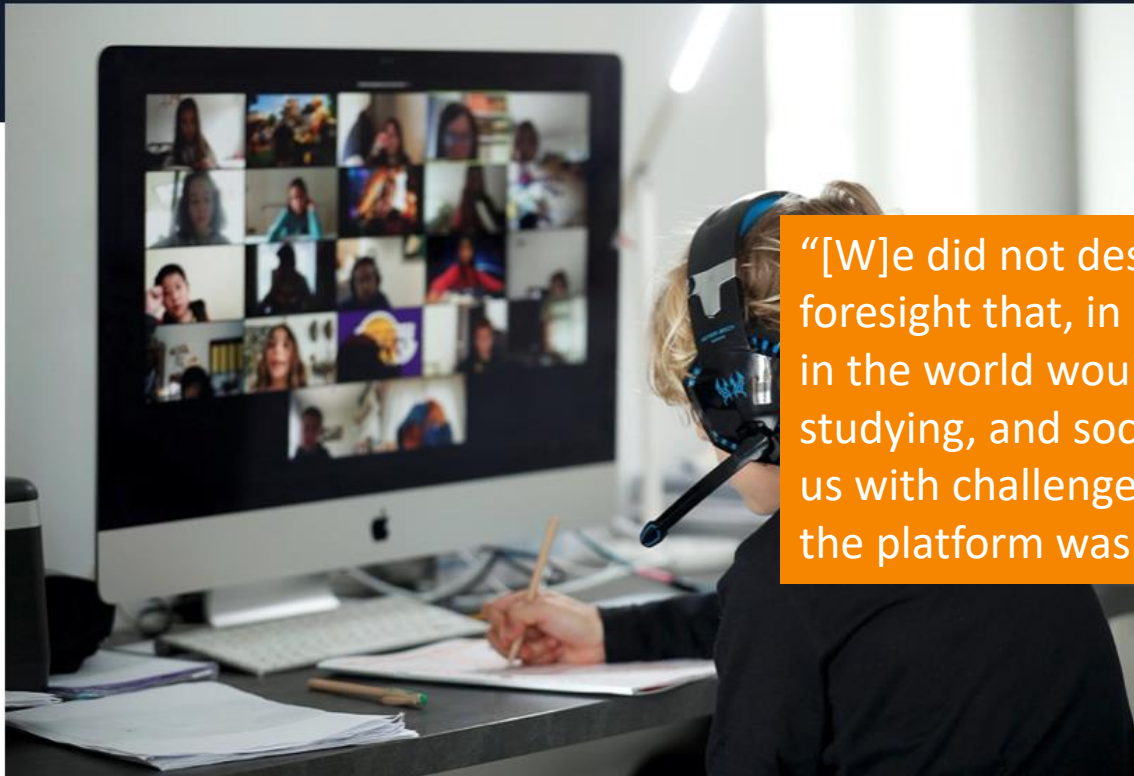
```
a@aol.com: | MeetingURL = https://us04web.zoom.us/j/ | HostKey =  
@gmail.com:W | MeetingURL = https://us04web.zoom.us/j/ | HostKey  
[@hotmail.com: | MeetingURL = https://zoom.com.cn/j/ | HostKey =  
e: | MeetingURL = https://us04web.zoom.us/j/ | HostKey =  
ail.com:1 | MeetingURL = https://us04web.zoom.us/j/50505550507 | HostKey =
```

“Chase, Citibank, educational institutions, and more”

# From 10M to 200M Users...

## 'Every day is a crisis': Zoom boosts its security as scrutiny grows

"We've got to double down on privacy, double down on security," Zoom CEO Eric Yuan said.



"[W]e did not design the product with the foresight that, in a matter of weeks, every person in the world would suddenly be working, studying, and socializing from home...presenting us with challenges we did not anticipate when the platform was conceived.



# FBI warns of 'Zoombombing' as more businesses, schools utilize teleconferencing

Cyber criminal

Posted: 6:12 PM, Apr

By: Tracy Carlos



Roundpixel Ltd

## 'Alcohol is soooo good': Trolls are breaking into AA meetings held on Zoom video calls and harassing recovering alcoholics

Aaron Holmes Mar 31, 2020, 1:22 PM



### 'Zoombombing' Becomes a Dangerous Organized Effort

Zoom, the videoconferencing app, has become a target for harassment and abuse coordinated in private off-platform chats.



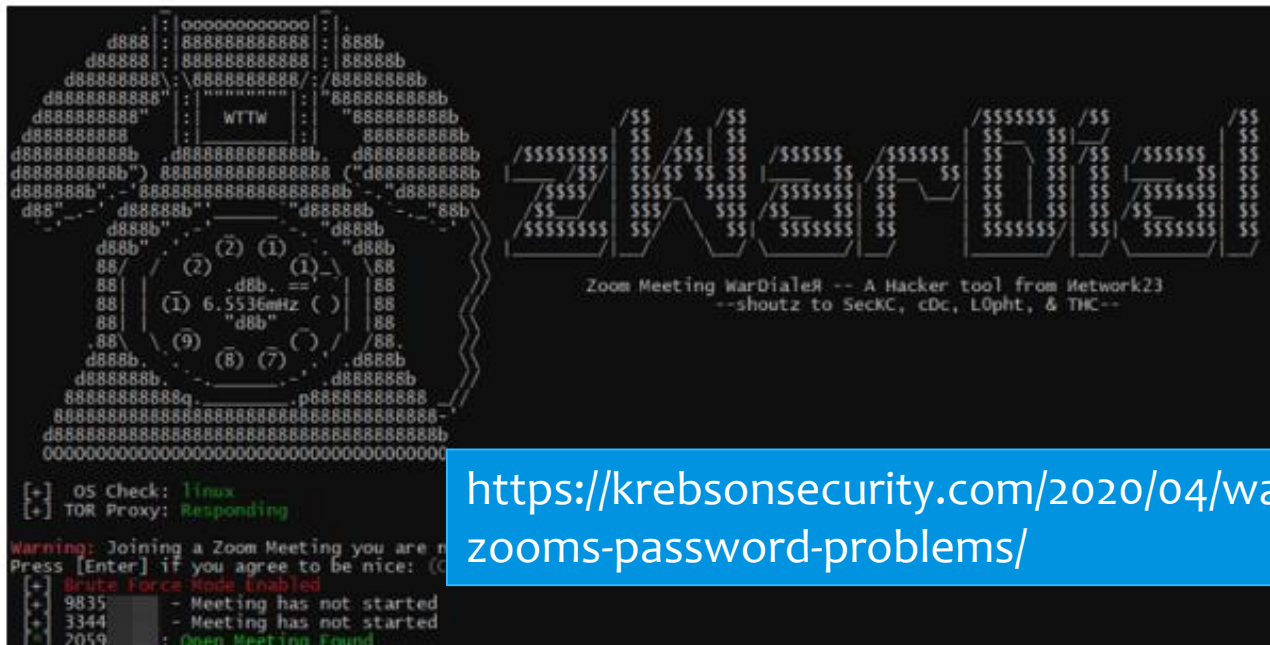
# Hackers “Scan” for Open Meetings

## 02 ‘War Dialing’ Tool Exposes Zoom’s Password Problems

APR 20  
**Problems**

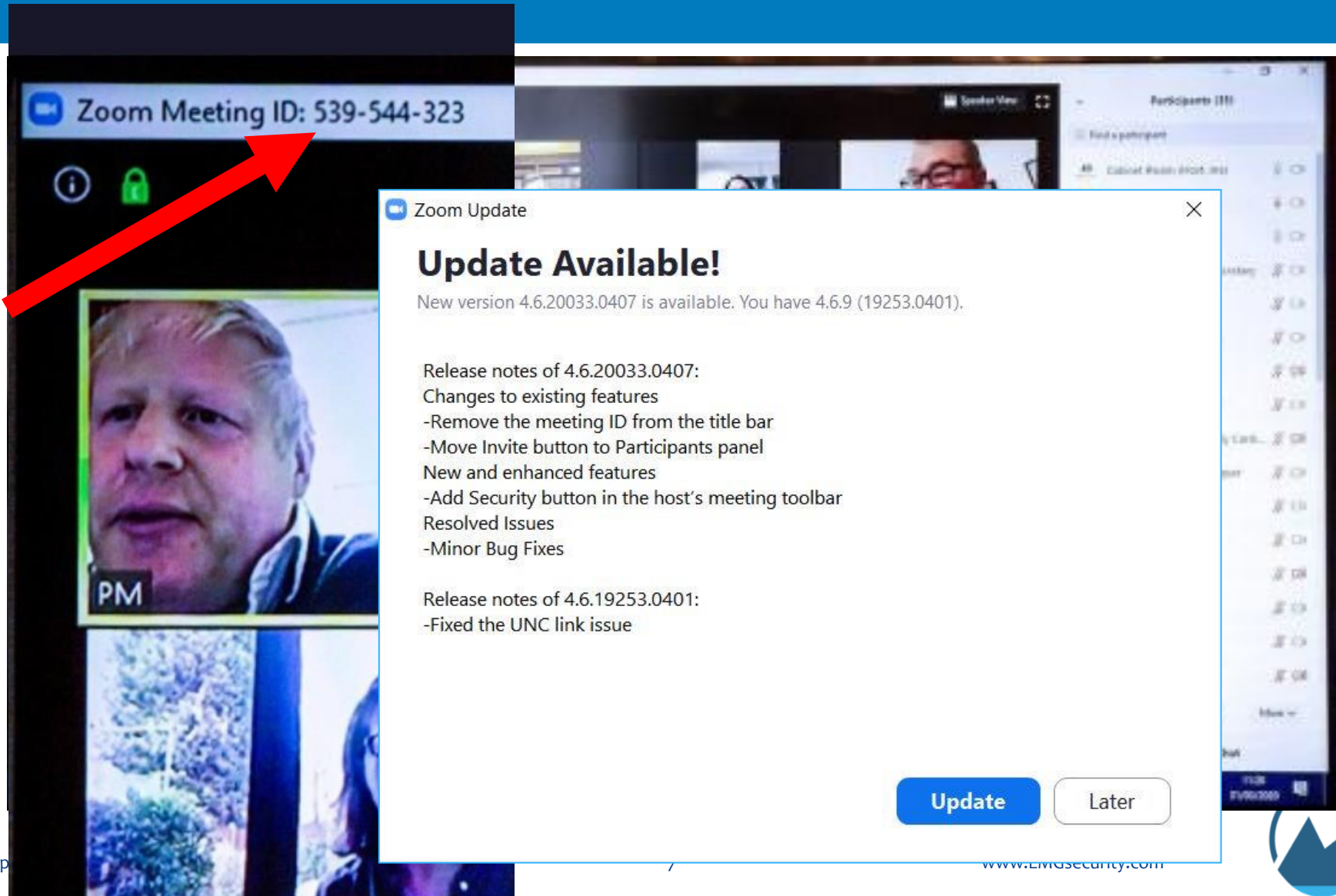
As the Coronavirus pandemic continues to force companies are now holding daily meetings using video without the protection of a password, there’s a decent “Zoom bombed” — attended or disrupted by someone data gathered by a new automated Zoom meeting discovery number of meetings at major corporations are not being

“[A] single instance of zWarDial can find approximately 100 meetings per hour, but ... multiple instances of the tool running in parallel could probably discover most of the open Zoom meetings on any given day.”



<https://krebsonsecurity.com/2020/04/war-dialing-tool-exposes-zooms-password-problems/>

# Human Error



The image shows a Zoom meeting window with a title bar displaying "Zoom Meeting ID: 539-544-323". A red arrow points to this ID. An "Update Available!" dialog box is overlaid on the meeting, listing release notes for versions 4.6.20033.0407 and 4.6.19253.0401. The dialog box includes buttons for "Update" and "Later".

**Zoom Meeting ID: 539-544-323**

**Zoom Update**

### Update Available!

New version 4.6.20033.0407 is available. You have 4.6.9 (19253.0401).

Release notes of 4.6.20033.0407:

- Changes to existing features
  - Remove the meeting ID from the title bar
  - Move Invite button to Participants panel
- New and enhanced features
  - Add Security button in the host's meeting toolbar
- Resolved Issues
  - Minor Bug Fixes

Release notes of 4.6.19253.0401:

- Fixed the UNC link issue

**Update** **Later**



# GotoMeeting-Bombing? (not as catchy)



The screenshot shows a GoToMeeting page for a user named 'boris johnson'. At the top left is the GoToMeeting by LogMeIn logo. The address bar contains the URL <https://www.gotomeet.me/borisjohnson>. Below the URL bar is a large white box with a grey circular profile icon containing a white silhouette of a person. Underneath the icon, the name 'boris johnson' is displayed in a sans-serif font. At the bottom of this white box is an orange button with the text 'JOIN MY MEETING'. Below the white box, there is a footer with links: [My GoToMeeting](#), [About Us](#), [Terms of Service](#), [Privacy Policy](#), and [Support](#). Below the links is a small line of text: 'All OpenVoice audio conferencing services are provided by LogMeIn Audio, LLC. LogMeIn Audio, LLC is the telecommunications provider and is responsible for the rates, terms, and conditions of the audio conferencing services. © 2019 LogMeIn, Inc. All rights reserved.'





# Move Fast and Roll Your Own Crypto

## A Quick Look at the Confidentiality of Zoom Meetings

April 3, 2020



### Protecting Your Data

Communications are established using 256-bit TLS encryption and shared content can be encrypted using AES-256 encryption.

This report examines the encryption that protects meetings in the popular Zoom teleconference app. We find that Zoom has “rolled their own” encryption scheme, which has significant weaknesses. In addition, we identify potential areas of concern in Zoom’s infrastructure, including observing the transmission of meeting encryption keys through China.

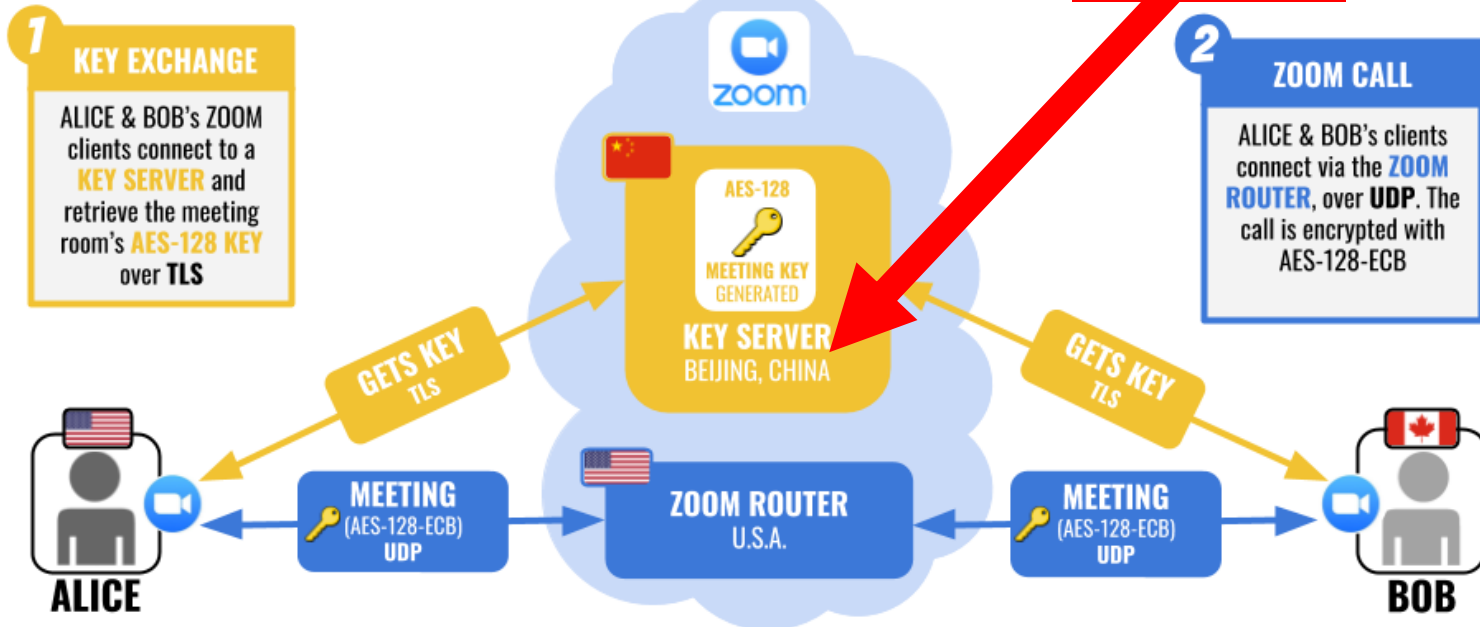
## Key Findings

- Zoom [documentation](#) claims that the app uses “AES-256” encryption for meetings where possible. However, we find that in each Zoom meeting, a single AES-128 key is used in ECB mode by all participants to encrypt and decrypt audio and video. The use of ECB mode is not recommended because patterns present in the plaintext are preserved during encryption.
- The AES-128 keys, which we verified are sufficient to decrypt Zoom packets intercepted in Internet traffic, appear to be generated by Zoom servers, and in some cases, are delivered to participants in a Zoom meeting through servers in China, even when all meeting participants, and the Zoom subscriber’s company, are outside of China.

# Geolocation

## OBSERVING A TEST ZOOM CALL

Beijing,  
China



**NOTE:** Citizen Lab observed these server locations during a test call. Other ZOOM calls may use servers and call routers in other locations.

<https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/>



## Zoom Lets Attackers Steal Windows Credentials, Run Programs via UNC Links

By [Lawrence Abrams](#)

March 31, 2020 11:59 PM 8



## 'Zoom is malware': why experts worry about the video conferencing platform

The company has seen a 535% rise in daily traffic in the past month, but security researchers say the app is a 'privacy disaster'



▲ Many, including the British prime minister, Boris Johnson, have been using Zoom during the coronavirus crisis. Photograph: Olivier Douliery/AFP via Getty Images

As coronavirus lockdowns have moved many in-person activities online, the use of the video-conferencing platform [Zoom](#) has quickly escalated. So, too, have concerns about its security.



**Dave Kennedy (ReL1K)**   
@HackingDave

Example of hyperbole for the Zoom discussion and horrid fear-mongering by the media and comments from individuals that are not even security researchers

This type of news is exactly what is damaging to the security industry and trust in us. [@guardian](#)

## Zoom isn't Malware.



Amit Serper [Follow](#)  
Apr 3 · 7 min read



Co-authored by: David Kennedy, founder TrustedSec, Binary Defense  
Amit Serper, VP Security strategy and principal security researcher, Cybereason

Russ Handorf, PhD. Principal Threat Intelligence Hacker, WhiteOps

This post is NOT sponsored by or affiliated with Zoom in any way.

Zoom is not malware. Zoom is safe to use for both you personally and businesses, but you should read through on how to best protect yourself and your company. Throughout the past few days, social media (mostly infosec twitter) is gushing with various opinions and hot takes about Zoom being malware due to multiple issues found with it. Some of these issues are indeed problematic (and are/were taken care of by Zoom) and some of the issues that are being raised and discussed in social media are in fact not bugs or issues with Zoom itself but issues with the way operating systems work.



# Zoom Security Checklist

- ✓ Ensure “Require a password when scheduling new meetings”, “Require a password for instant meetings”, and “Require password for participants joining by phone” are on.
- ✓ Turn off “Embed passwords in meeting link for one-click join”
- ✓ Ensure “Use Personal Meeting ID when scheduling a meeting” and “Use Personal Meeting ID when starting an instant meeting” are off.
- ✓ Don’t post meeting links to public places.
- ✓ Utilize the “waiting room” feature to ensure only authorized users join the call.
- ✓ Ensure “Join before host” is disabled.
- ✓ Restrict remote control to host only.
- ✓ Make sure hosts are familiar with “mute,” “hold” and similar controls.
- ✓ Use a strong password, a minimum of 14 characters.
- ✓ Utilize MFA whenever possible.
- ✓ Utilize a full-tunnel VPN to protect users.
- ✓ [Restrict NTLM through GPO.](#)
- ✓ Ensure users have strong endpoint protection.



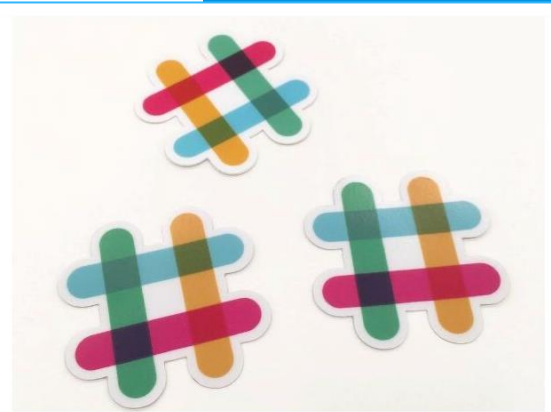
# Beyond Zoom: How Safe Are Slack and Other Collaboration Apps?



Author:  
Tara Seals

April 6, 2020 / 5:49 am

COVID-19's effect on work footprints has created an unprecedented challenge for IT and security staff. Many departments are enabling collaboration apps for all — but without proper security can be a big risk.



Cyber Security News Hacking News News Vulnerabilities

## Slack Patch Critical Vulnerability Allowing Automated Account Takeovers

March 17, 2020 Abeerah Hashim 990 Views account takeover, Accounts Hijacking, bug, Bug Bounty, bug

## High-Severity Cisco Webex Flaws Fixed



The high-severity flaws, existing in Webex Player and Webex Network Recording Player, can allow arbitrary code execution.

mssecurity.com



# “What About Microsoft Teams?”

- Very advanced compliance options
  - ISO 27001, ISO 27018, SSAE16, SOC1, SOC2, HIPAA EU Model Clauses (EUMC)
- Regional data allocation (Americas, UK, EU, Middle East & Africa, APAC).
- FIPS-compliant encryption key exchange
- Encryption at rest & transit
- Installer/update vulnerability
  - <https://nvd.nist.gov/vuln/detail/CVE-2019-5922>





# Cloud Cybersecurity Checklist

1. Access and Sharing
2. Authentication
3. Encryption
4. Ownership
5. Location
6. Backups
7. Monitoring and Logs
8. Termination of Service
9. Security Assessments
10. Compliance
11. Incident & Breach Response



# Daily Registration of new "Zoom" Domains

120

100

80





Re:SAFTY CORONA VIRUS AWARENESS WHO

WO World Health Organization



Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Safety measures

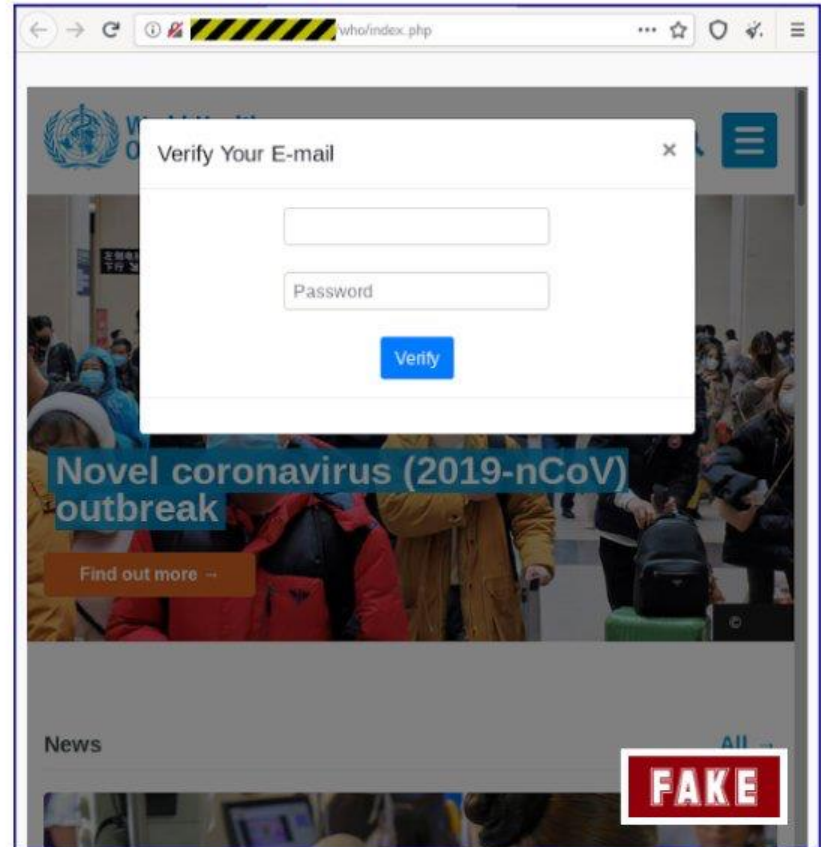
Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong  
Specialist wuhan-virus-advisory

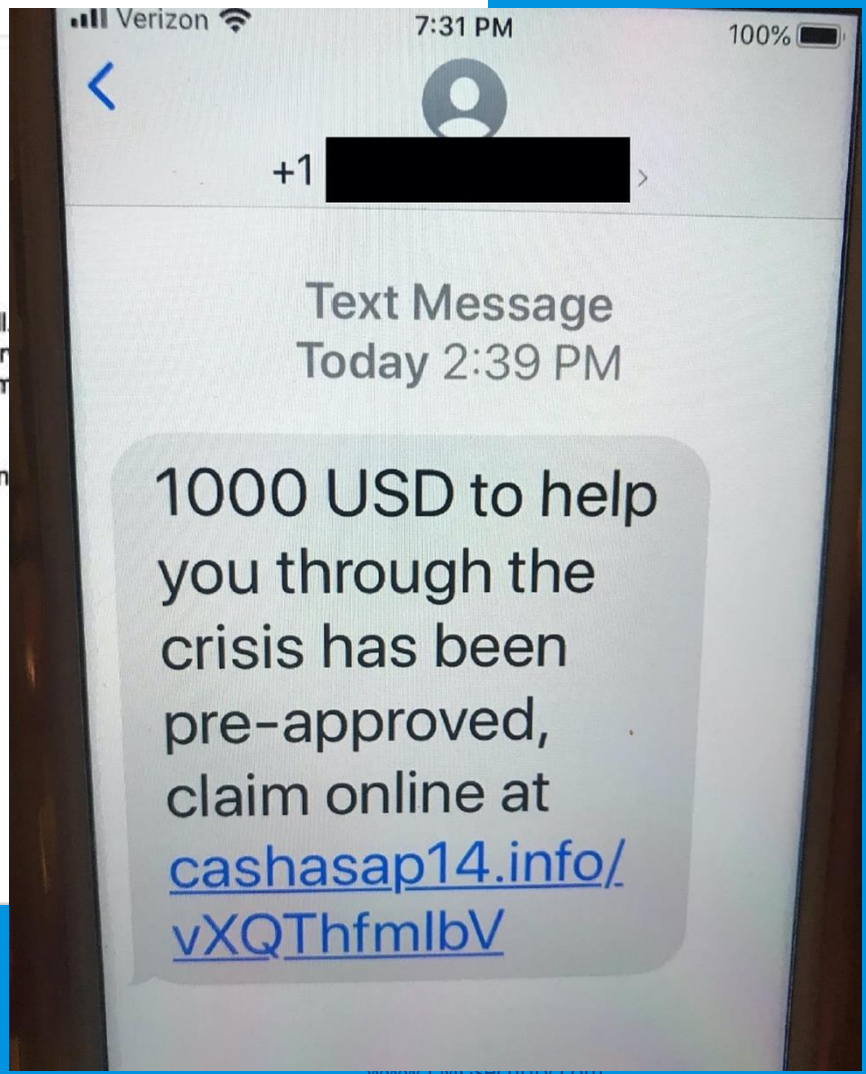
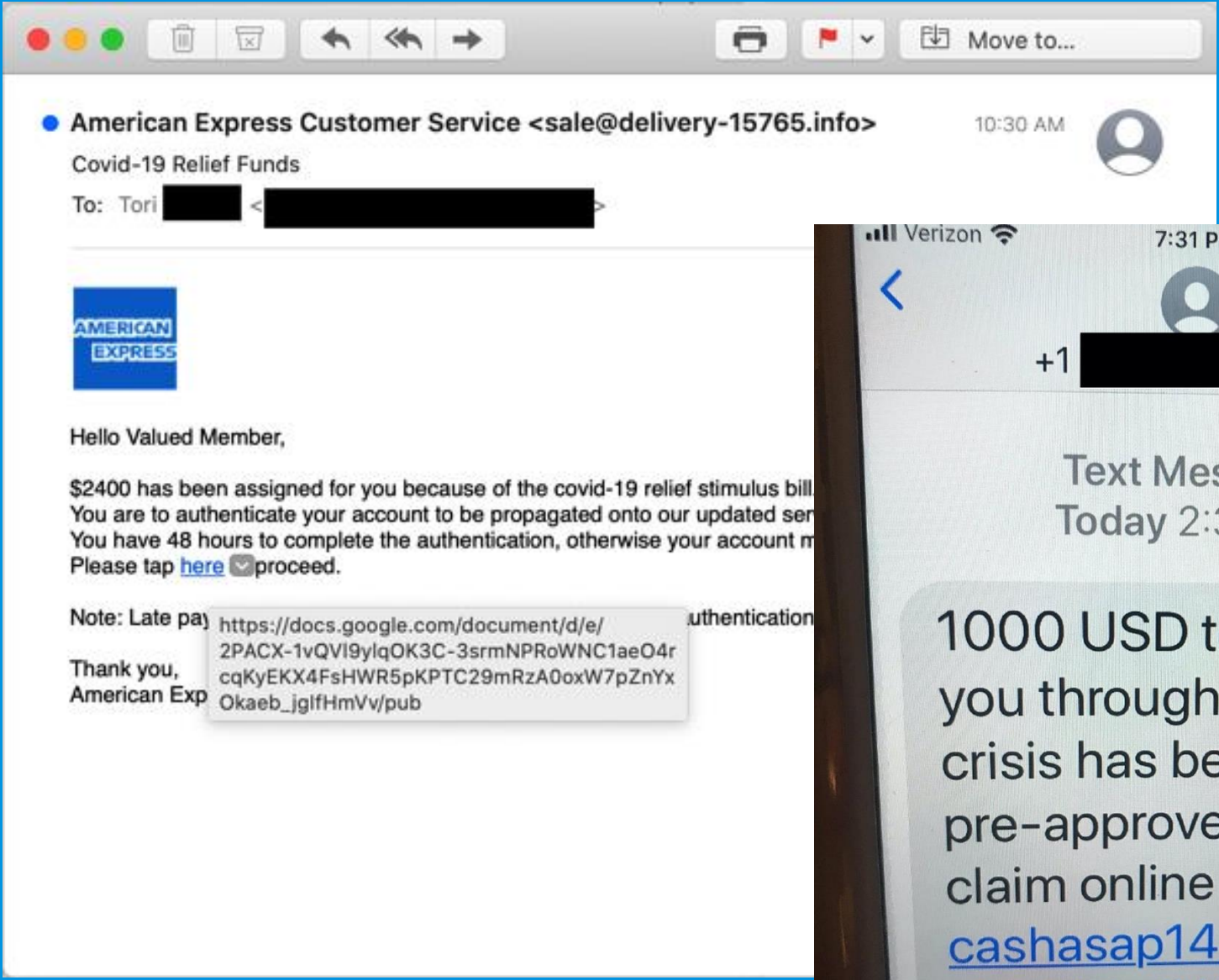
**FAKE**

COVID-19 phishing impersonating the WHO



WHO-themed phishing site

<https://www.bleepingcomputer.com/news/security/world-health-organization-warns-of-coronavirus-phishing-attacks/>



# Remote Work Scams

**From:** "[imgsecurity.com VR](#)" <[gNdes@zoo.ox.ac.uk](mailto:gNdes@zoo.ox.ac.uk)>  
**Subject:** **Imgsecurity 3 Missed Call - Ref: AhwMq**  
**Date:** April 1, 2020 at 1:30:23 PM MDT  
**To:** [news@imgsecurity.com](mailto:news@imgsecurity.com)

Message from Trusted server.

## Office 365 Voice-Mail

Dear news:

You have an incoming voice-message in your voice-portal  
as of Wednesday 11, March 2020.

You can listen or download here .

[Listen/Download](#)



# Product Scams - Masks

**From:** "Alice" <Kmdohealth@163.com>  
**Subject:** Re:Re:mask order  
**Date:** March 26, 2020 at 3:28:26 PM MDT  
**To:** <info@imgsecurity.com>  
**Reply-To:** <Kmdohealth@163.com>

Dear friend,

How are you? First, I wish you have a good health.

I am Alice who Mainly supplies three layer masks, KN95 FFP2, FFP3 masks, Infrared Thermometer, temperature gun, disposable gloves; Protective clothing, protective masks and other protective materials.

We are big factory located in Shenzhen China, producing Thermometer and Face Mask, these days, we get many enquiry and bulk quantity orders from many different countries,

I wonder if i can hlep you? If you want a trail order,feel free email me.

**From:** "Ivy" <asianmask\_china@163.com>  
**Subject:** surgical masks  
**Date:** March 21, 2020 at 4:06:48 PM MDT  
**To:** <training@imgsecurity.com>  
**Reply-To:** <asianmask\_china@163.com>

Dear sir,

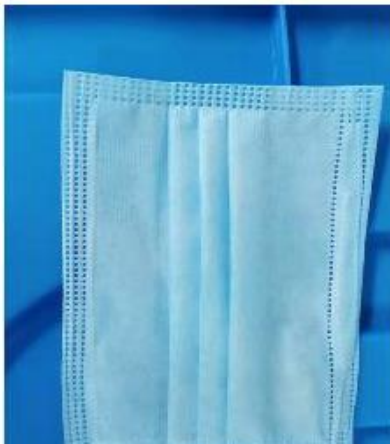
Good morning. i am Ivy from Professional mask factory.and we can supply sanitizer gel.

First, I wish you have a good health, recently the virus spread seriously, so we everyone

Our products include General surgical masks and professional surgical masks.

The efficiency of bacterial filtration is at least 95%. ( BFE 95)

The Picture is our Disposable surgical mask.





## Due to the recent outbreak for the Coronavirus, the World Health Organization is giving away vaccine kits. Just

You just need to add water, and the drugs and vaccines are ready to be added. The kits contain pellets containing the chemical machinery that synthesises the end product. The kits also contain instructions that tell the drug which compound to create. Mix two parts together in a vial and you are ready.

ORDER NO

## HERE ARE WHAT RECENT USERS ARE SAYING

### Guido Zambrano Torre



The coronavirus probably has a stronger ability to spread than the World Health Organization has estimated so far.

### Magdaliza Negreira



Our review shows that the coronavirus is at least as transmissible as the SARS virus. And that says a great deal about the seriousness of the situation.

### Mitch and Stacey

The World Health Organization

### Isabel Jara



The higher the number, the more transferable the virus is and the higher the risk for rapid spread. When the reproduction number falls below 1.0, the epidemic is likely to die out.

### Albert Jing



The studies consisted of estimations of the growth rate based upon the cases observed in the Chinese population, and based upon statistical and mathematical methods.

### Melissa Grafster

# Phone Scams



# FBI: COVID-19-Themed Business Email Compromise Scams Surge

Fraudsters Keep Trying to Turn Pandemic to Their Advantage

Ishita Chigilli Palli (@Ishita\_CP) · April 7, 2020



Microsoft Corporation [US] <https://login.live.com/login.srf?wa=wsignin1.0&>



## Sign in

Use your work or school, or personal Microsoft account.

Keep me signed in

Sign in

No account? [Create one!](#)

Office 365 Outlook

invoice

Exit search

In folders

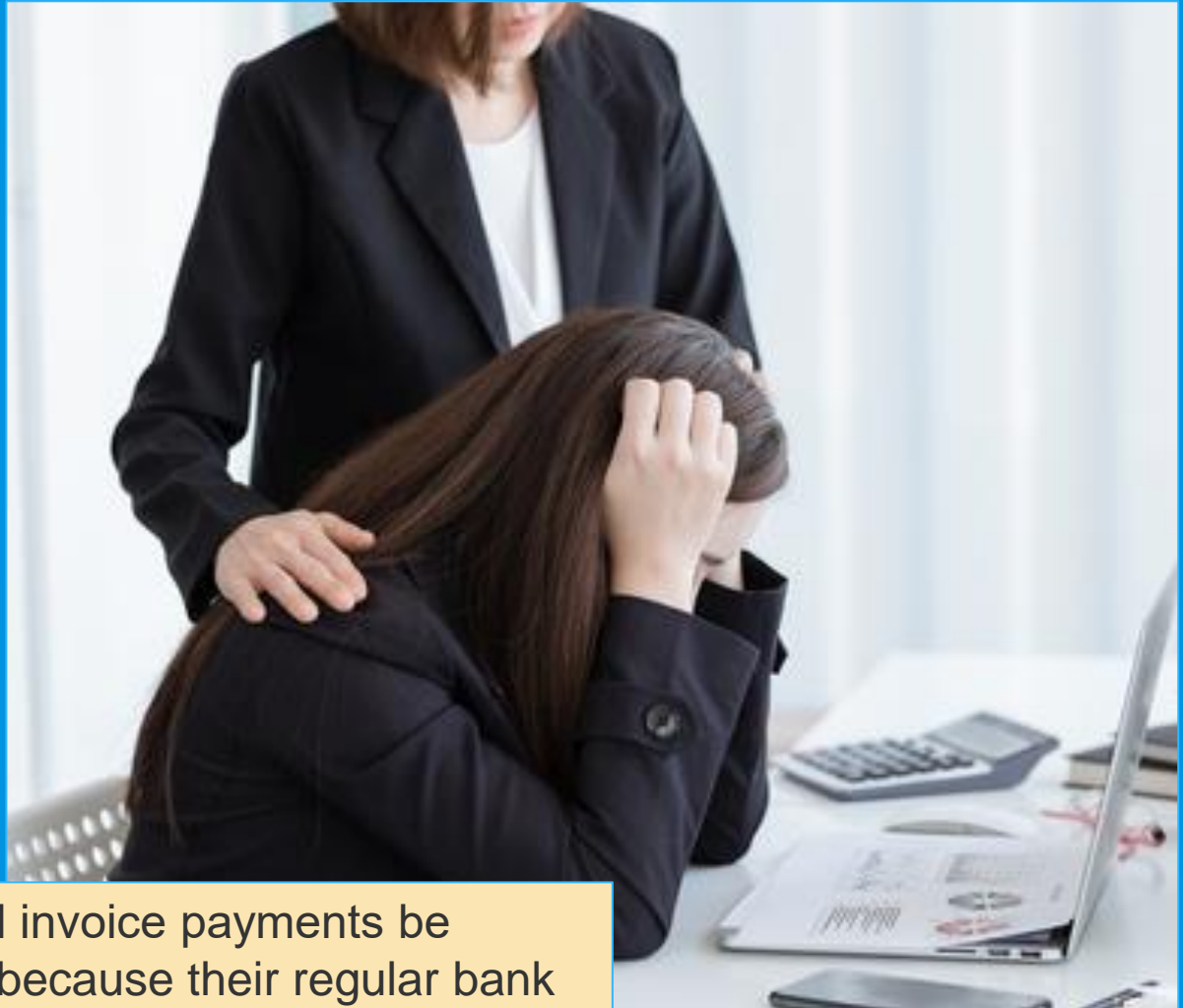
All folders

Top results

New



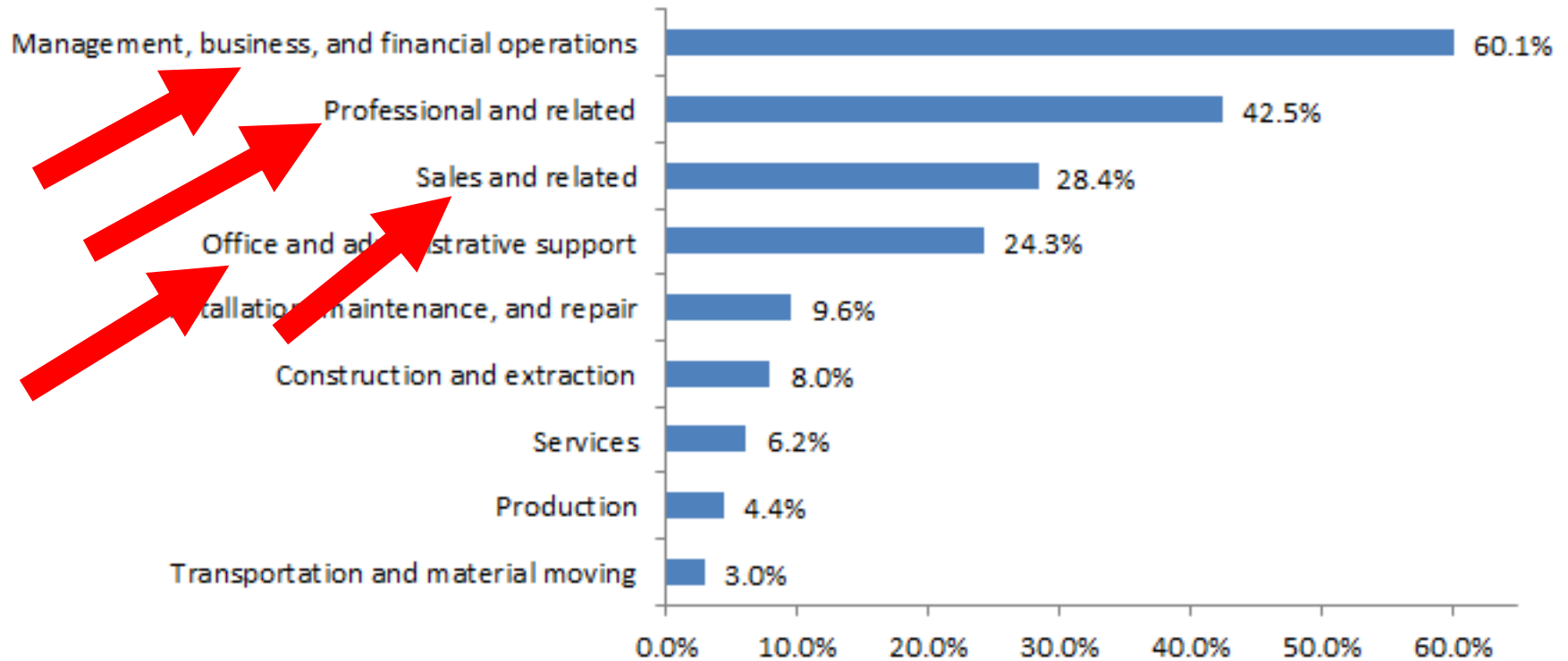
demic to ramp-up business  
warned this week.



“The client requested that all invoice payments be changed to a different bank because their regular bank accounts were inaccessible due to **“Corona Virus audits.”** The victim sent several wires to the new bank account for a significant loss before discovering the fraud.”



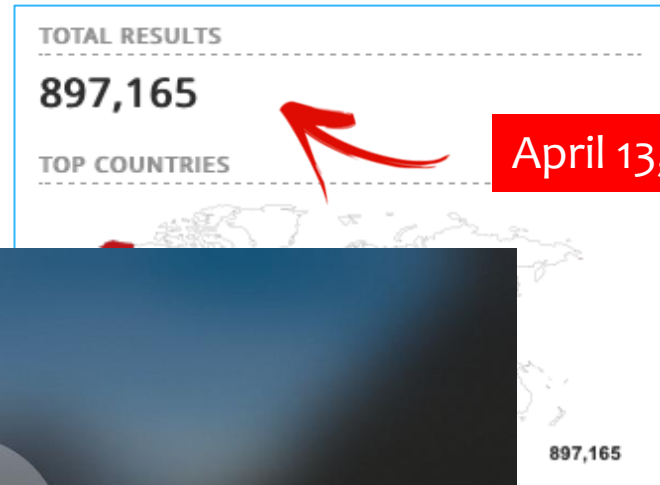
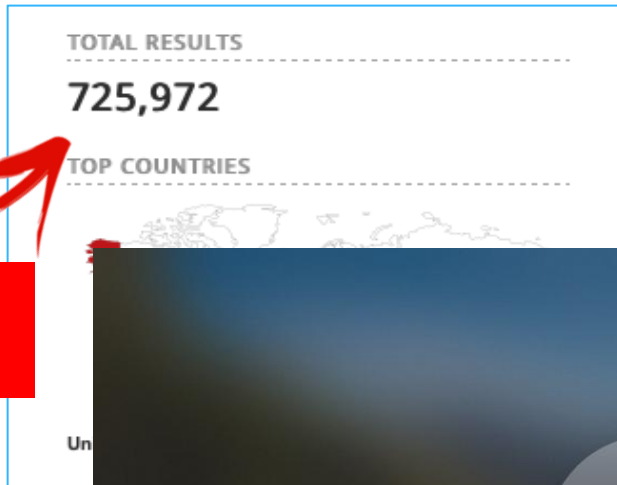
# Share of workers who can telework, by occupation



Source: The American Time Use Survey from BLS, <https://www.bls.gov/news.release/flex2.t01.htm>

Released Sept 2019

# Going Up: Exposed Login Interfaces



## Ransomware Gangs' Not-So-Secret Attack Vector: RDP Exploits

But RDP Attack Overuse Leads Other Hackers Back to Botnets, Researchers Find

Mathew J. Schwartz (@euroinfosec) · November 4, 2019

RD  
339  
Cit  
SM  
TC  
McAfee Skip the password  
Microsoft App

2,721  
707  
52  
23

security.com



# Insecure Defaults

Microsoft Azure Search resources, services, and docs (G+/)

Home > Virtual machines > Create a virtual machine

Create a virtual machine

RDP (3389)

**⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.**

only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Review + create < Previous Next : Disks >



# Stolen Credentials

## HACKED WINDOWS REMOTE DESKTOP (RDP / VPS)

<b>Vendor</b>	Skyscraper (1900) (4.94★) (a 210/1/1) (🚫 23/0/0)
<b>Price</b>	฿0.00241 (\$15.6)
<b>Ships to</b>	Worldwide, Worldwide
<b>Ships from</b>	Worldwide
<b>Escrow</b>	No



OP) with A

Question Report

Quantity: 1

coin (BTC)

Buy Now

Views 10

cheap price!

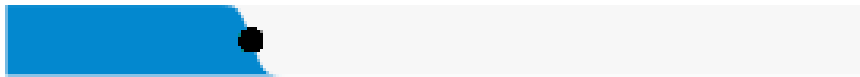


# How Hackers Break In

Phishing



Use of stolen creds



Top Threat action varieties in breaches, *Verizon Data Breach Investigations Report 2019*

“Hackers don’t  
break in, they log in”

- Bret Arsenault, Microsoft



# Akamai: We Saw 61 Billion Credential Stuffing Attacks in 18 Months

ED TARGETT EDITOR  
13TH SEPTEMBER 2019

+ INCREASE / DECREASE TEXT SIZE -



## 'Collection #1' reveals 773 million email addresses, passwords in one of largest data breaches ever

You can check to see if your username and password have been leaked.

Mark Hachman (PC World (US online)) on 18 January, 2019 08:25

0 Comments



Add to favorites



# Authentication Methods

- Something you know (Type 1)
- Something you have (Type 2)
- Something you are (Type 3)
- Multifactor = more than one



## Online Banking Login

Username:   
Password:

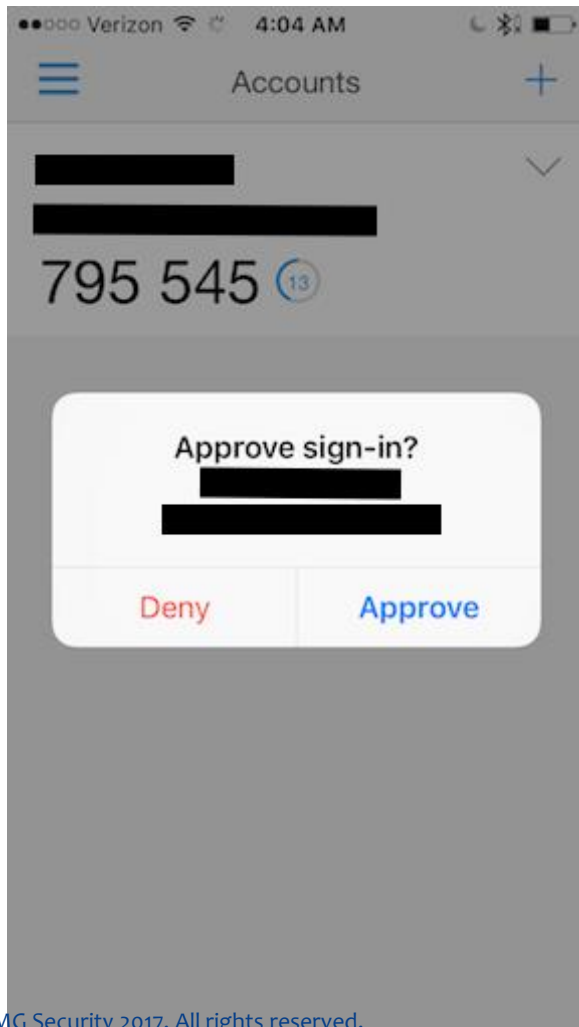
- New user
- Forgot pass

If this is the first time as a new user, blank and check

- ▶ New Users Sign
- ▶ Try Our Demo
- ▶ More Informat



# Authenticator Apps



- Cheap & easy options
- Office365
- Google
- Duo

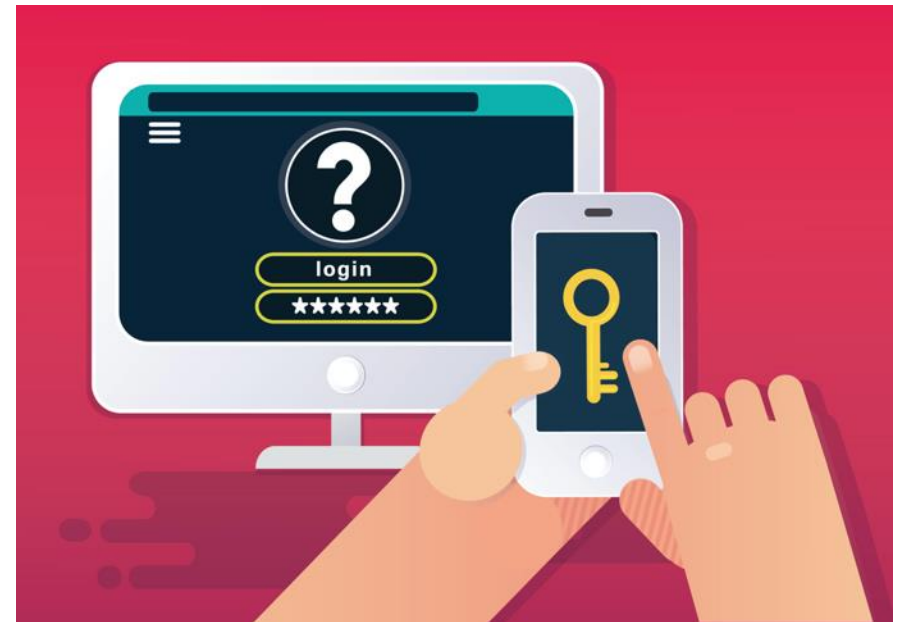
▪ [www.LMGsecurity.com/passwords](http://www.LMGsecurity.com/passwords)





# 2FA Best Practices

- Use **strong** 2FA (ie an app)
  - How-to videos are here:  
<https://imgsecurity.com/passwords>
- Turn off SMS-based authentication
- Check that your cloud providers support strong authentication



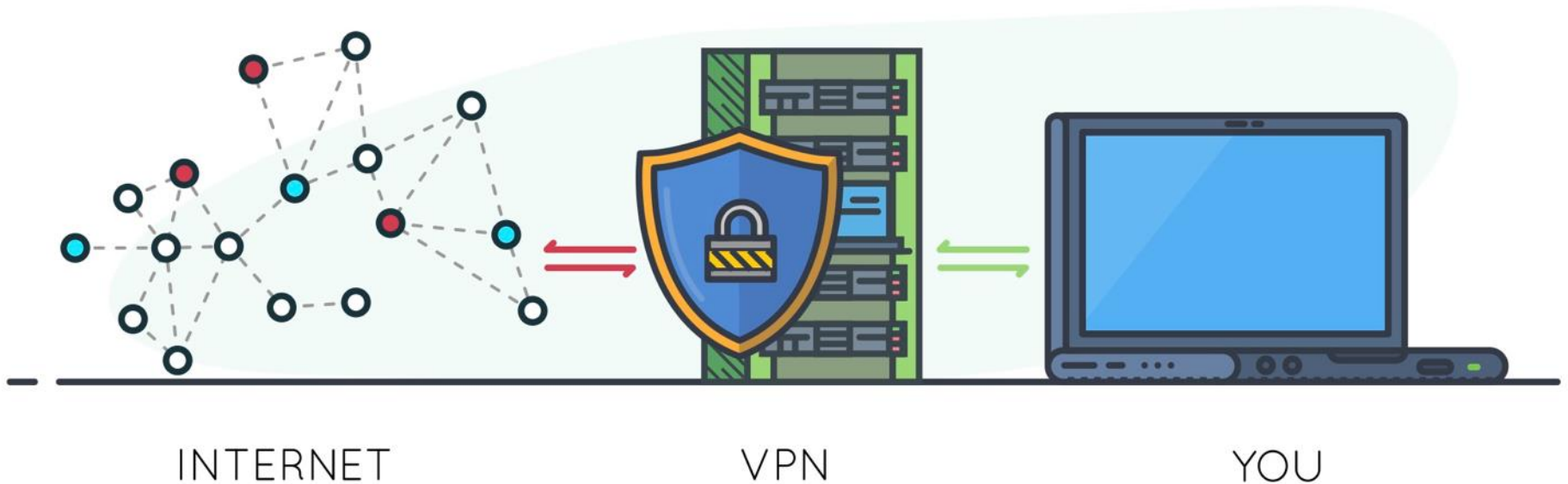
“Not All Two-Factor Authentication is Created Equal”

<https://www.LMGsecurity.com/not-all-two-factor-authentication-is-created-equal/>



# Use A VPN

- Prevent server exposure
- Encrypt your communications
- Scan remote devices for patches & A/V
- Split tunnel vs. full tunnel
- Segment



# Security Cleanups & Configuration Checks

- Security Cleanups!
- Virtual Desktop Infrastructure (VDI)
- Virtual Private Cloud (VPC)
- VPN Configuration
- Perimeter port scanning



<https://www.LMGsecurity.com/remote-security/>





aim for  
**PROGRESS**  
not  
**PERFECTION**

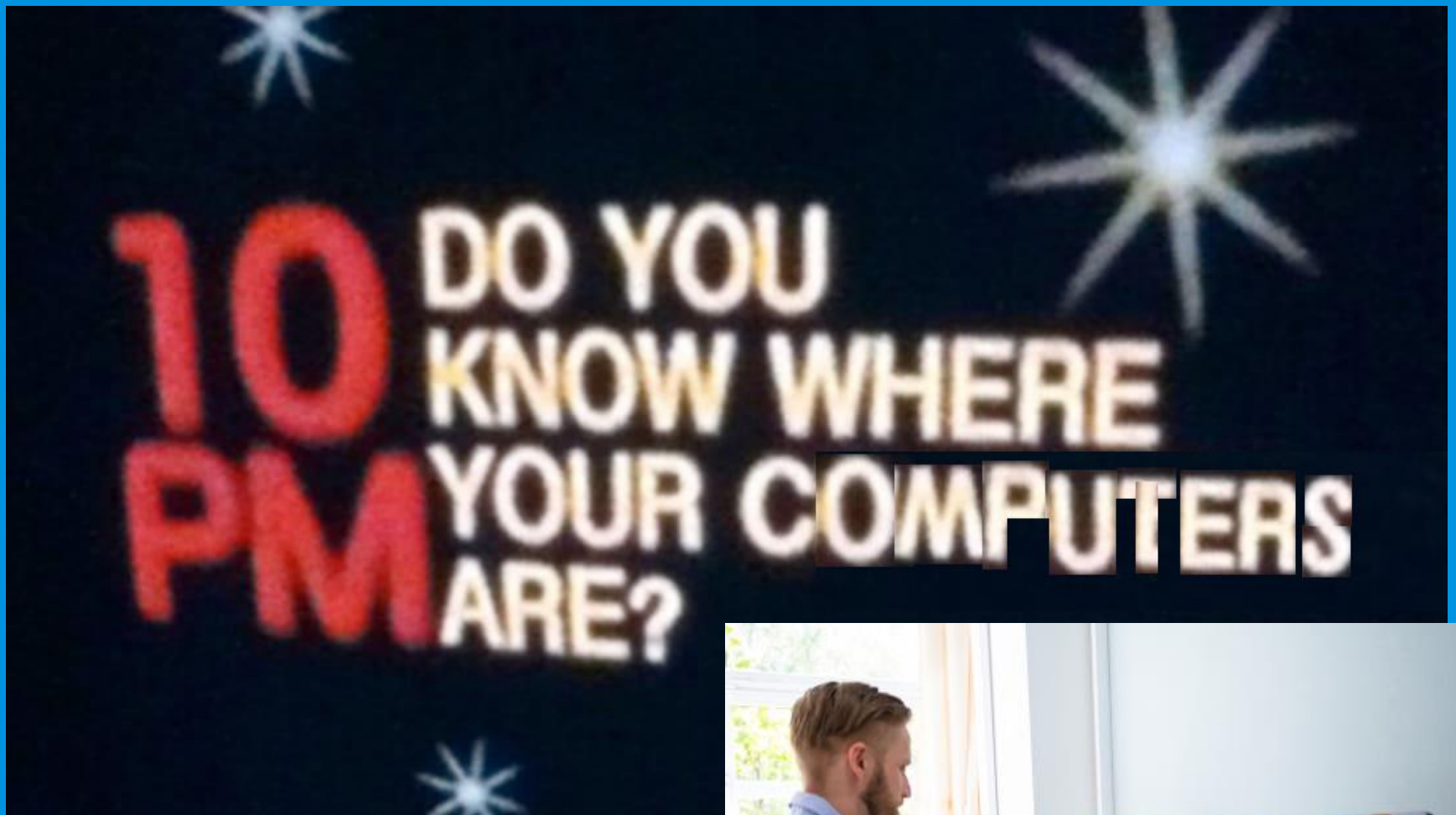
# The Coronavirus Is Creating a Huge, Stressful Experiment in Working From Home

Even before the pandemic struck, remote work was accelerating in the U.S. But the next few months will be a very strange test of our white-collar future.

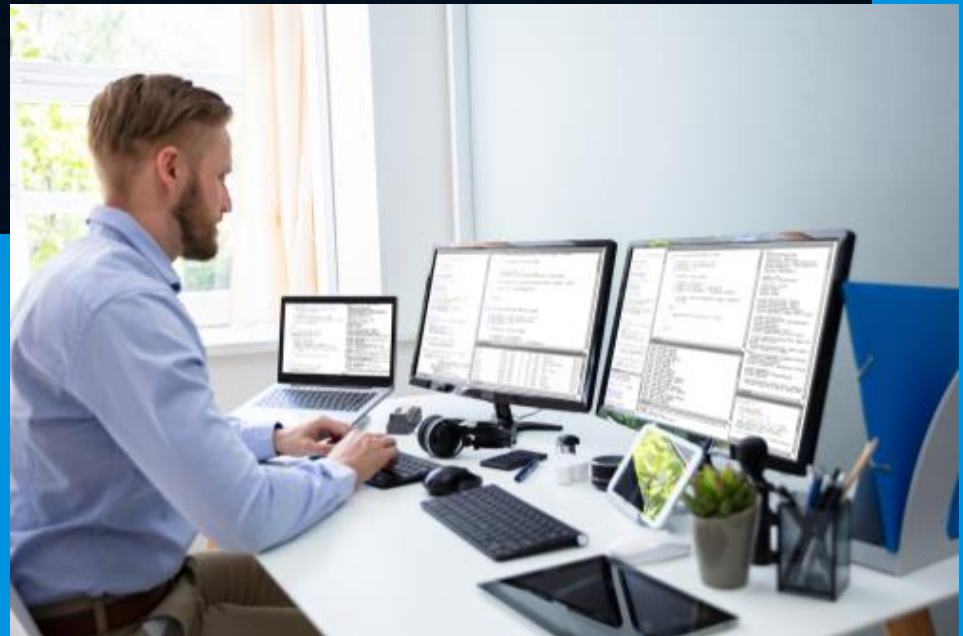
MARCH 13, 2020



- Asset Management
- Physical Security Challenges
- Access Control
- BYOD
- & More



<https://www.mentalfloss.com/article/30945/origin-its-10-pm-do-you-know-where-your-children-are>



# Asset Management

- Employees have brought home equipment
  - Monitors
  - Computers
  - Keyboards & Mice
  - Desks & Chairs
  - Locks etc





# Asset Management

- Keep track!
  - Survey
  - Checkout system
  - Periodic checks (don't wait 4 months)
- New equipment
  - I.e. No sharing headsets
- Consider what happens w/ furloughs/layoffs





# Define Your Workspace & Communicate Boundaries



Sharing != Caring

Set a password & PIN

Screen locking



**Spy**





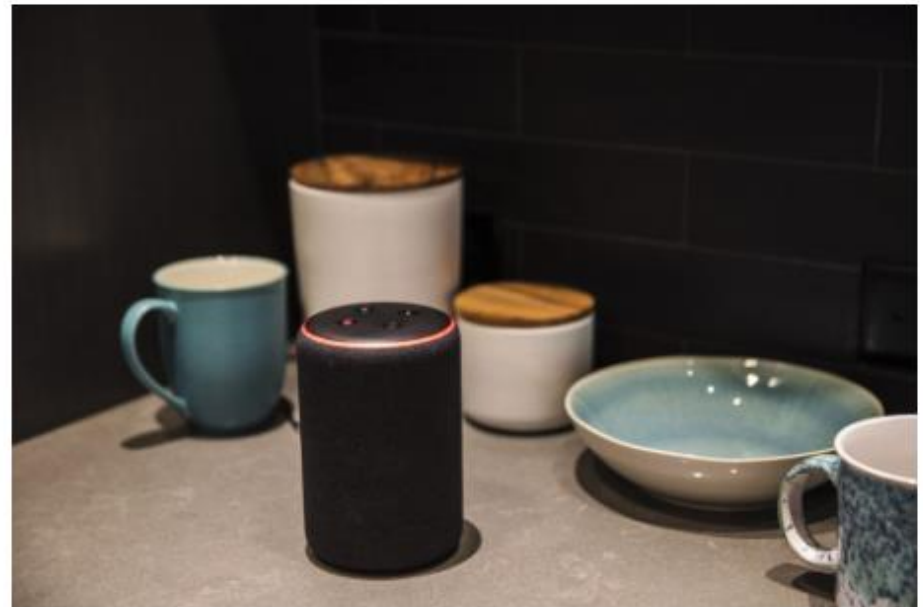
# “What About Active Listening Devices Like Alexa/Google Home?”

- “What’s a good policy for active listening devices in an employee’s home, like Alexa or Google Home?”
- Activate accidentally 1.5 to 19 per day
- Consider going to a different room for sensitive conversations

<https://moniotrlab.ccis.neu.edu/smart-speakers-study/>

## Locked-Down Lawyers Warned Alexa Is Hearing Confidential Calls

By [Crystal Tse](#) and [Jonathan Browning](#)  
March 20, 2020, 10:59 AM MDT

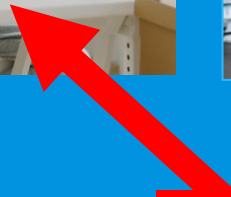
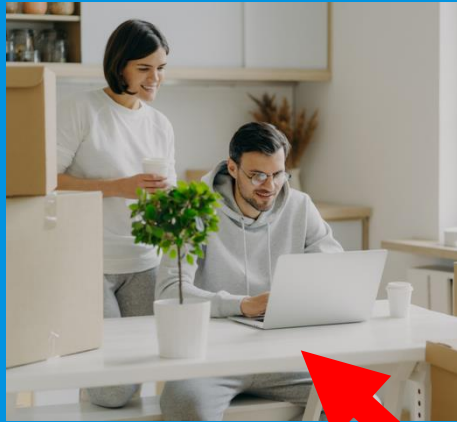


An Amazon Echo Plus smart speaker. *Photographer: Andrew Burton/Bloomberg*

Hey Alexa, stop listening to my client’s information.







Clear Policies

NDA?



Use Locks

Do Not Write  
Down  
Passwords

Clean Desk  
Policy

# Lost/Stolen Devices

## A Stolen Laptop Contained Data For More Than 114,000 Patients At Truman Medical Centers

By DAN MARGOLIES • DEC 18, 2019

A spokeswoman for the hospital said the laptop was stolen from an employee's vehicle.



A spokeswoman for the hospital said the laptop was stolen from an employee's vehicle.

BIGSTOCK

- Laptop stolen from vehicle
- Data breach
- “Password-protected”
  - Unencrypted?
- Rapid deployment = errors







# Lost/Stolen Devices - Defense

- Policy
  - Sample policy template!
  - <https://www.LMGsecurity.com/resources/remote-work-policy-template/>
- Encryption
- Laptop locks
- Training
- Clear reporting process





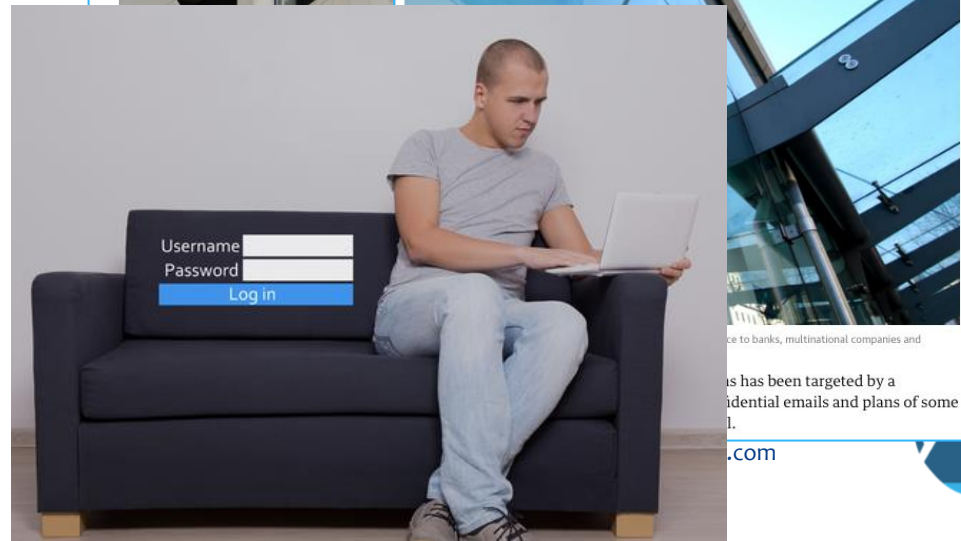
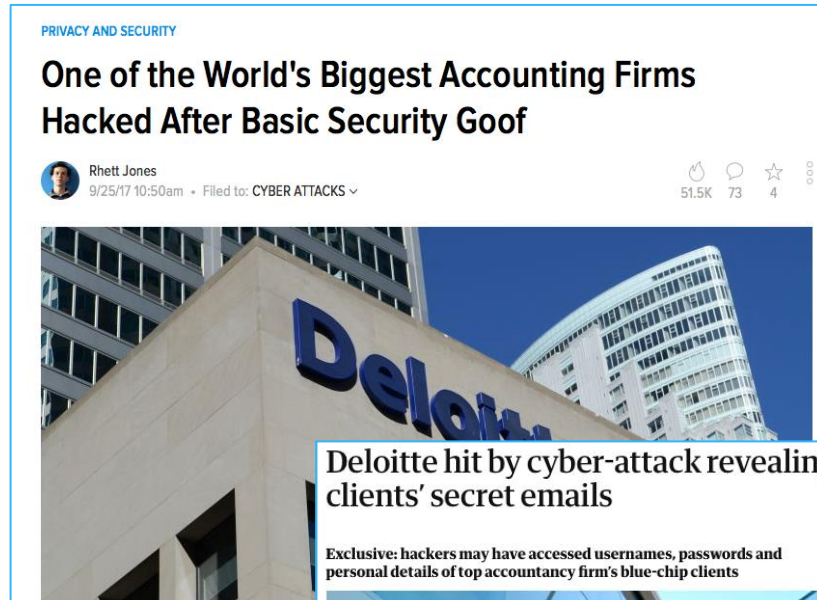
# Remote Work Security Tips for Employees

- **Know your organization's remote work policies and follow them.**
- **Watch out for phishing emails and phone scams.**
- **Define your physical workspace** and communicate boundaries.
- **Do not share computers or mobile devices that contain sensitive data** with family members or roommates.
- **Set a strong password or PIN** for all devices. Do not re-use passwords.
- **Use a password manager.**
- **Use MFA.**
- **Lock your screen whenever you step away from your computer**, particularly if you are in a shared living space.
- **Use a privacy screen** to help prevent unauthorized access.
- **Use locks when possible**, such as lockable doors or storage spaces.
- **Maintain a clean desk.** Even if employees do not have locks, putting sensitive information out of sight helps to protect it from accidentally being viewed.
- **Secure your home wireless network.**
- **Follow your organization's secure disposal policies.**
- **Do not copy sensitive work data to your personal computers or mobile devices** without authorization.
- **Keep track of what company devices/furniture you have at home.** Provide this information to your company proactively, if possible.
- **Immediately report anything suspicious** to an appropriate contact at your organization.

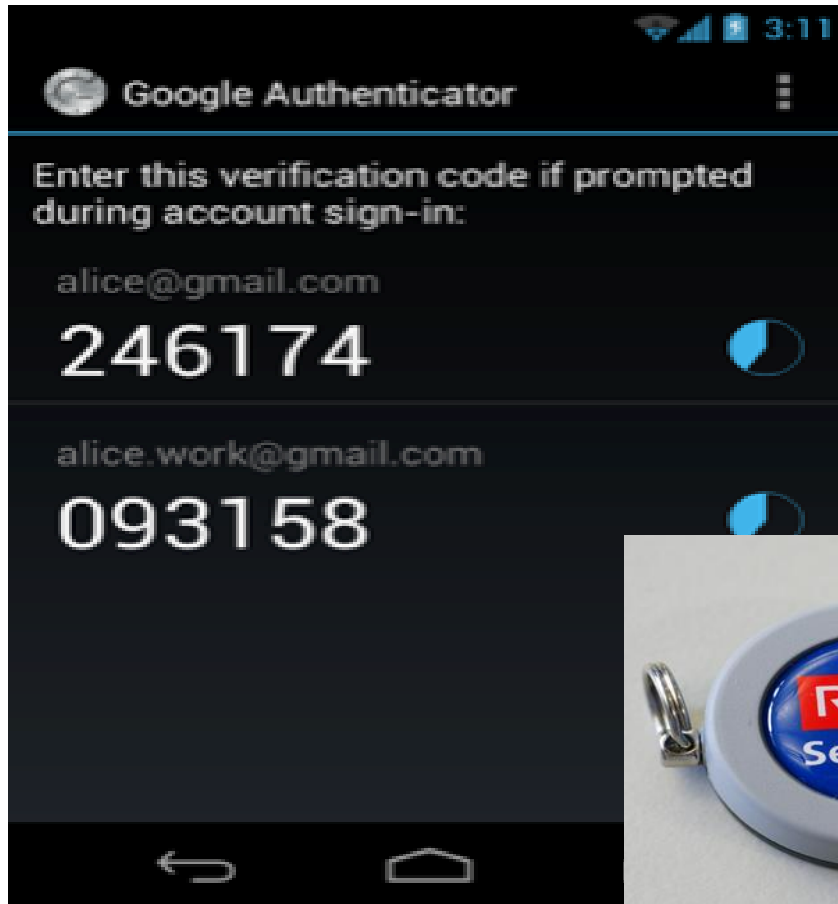


# Emergency BYOD

- Different risk model
- Higher-risk web surfing
- Games, utilities, unknown apps
- Maybe no antivirus
- No continuous monitoring
- Case: Biomedical company
  - IT admin used home computer
  - Pwd saved in Chrome
  - Infected
  - Ransomware & data theft
  - Major operational damage



# Remember: Multi-Factor Authentication



Login codes from authenticator apps for Android (left) and Windows Phone



# “How Secure Are Cloud Storage Vendors?”

- “How secure are the cloud storage vendors like DropBox and Microsoft OneDrive?”
- Varies a lot
- Terms of Service
- Vulnerabilities/Hacking
- Stolen Passwords

## Dropbox's Big, Bad, Belated Breach Notification

69 Million Dropbox Passwords Compromised; Last.fm Reportedly Breached in 2012

Mathew J. Schwartz (@euroinfosec) · September 1, 2016

   [Twitter](#) [Facebook](#) [LinkedIn](#)  Credit Eligible [Get Permission](#)



**Only as secure as their users!**



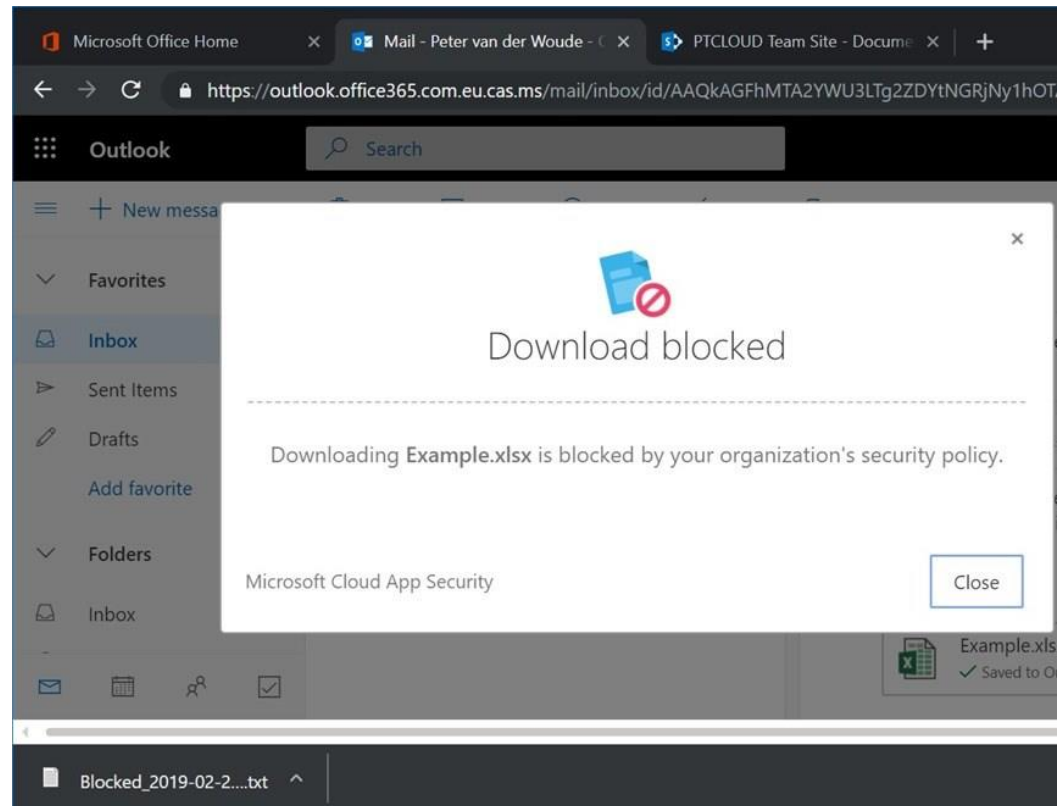
# Where is Your Data?

- Downloads from cloud/email
- Send to personal email/cloud
- USBs
- Printers
- Spyware/malware concerns
- Lack of proper encryption
- Coronavirus furloughs/layoffs?



# Restrict Downloads

- Require use of approved cloud storage
- Restrict downloads when used from:
  - Unmanaged devices
  - IP Address/Location

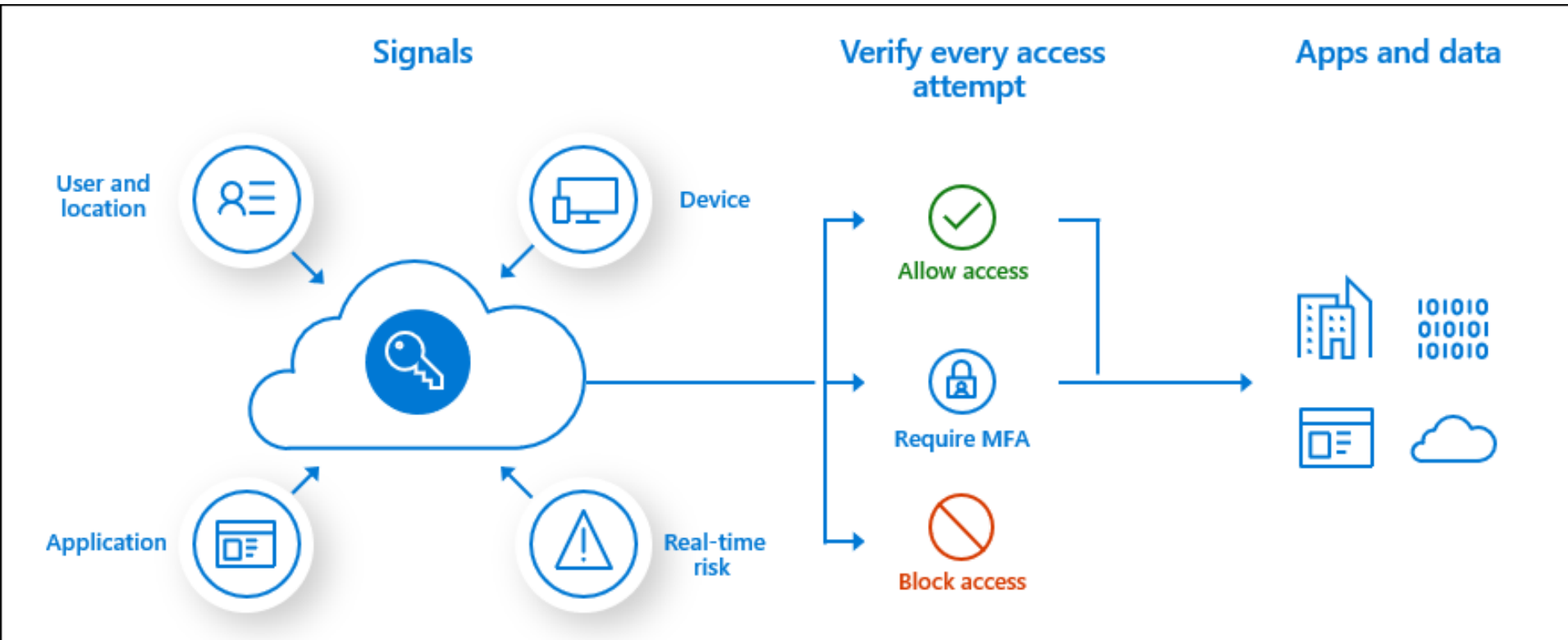


<https://i1.wp.com/www.petervanderwoude.nl/wordpress/wp-content/uploads/CAS-Example-EXO02.jpg?ssl=1>



# Enable Cloud Security Features

- Microsoft Azure's "Conditional Access":





# Mobile Device Management (MDM)

- Remote Wiping of Data
- Location Tracking
- Antivirus
- Policy Enforcement
  - Screen locking
  - PINs
- Etc.



# Emergency BYOD Checklist

## For IT

- ✓ Establish policies
- ✓ Require a PIN/passcode
- ✓ Implement MFA
- ✓ Deploy antivirus
- ✓ Enable cloud security features
- ✓ Restrict downloads
- ✓ Consider MDM deployment
- ✓ Distribute physical security tools
- ✓ Publish incident reporting hotline



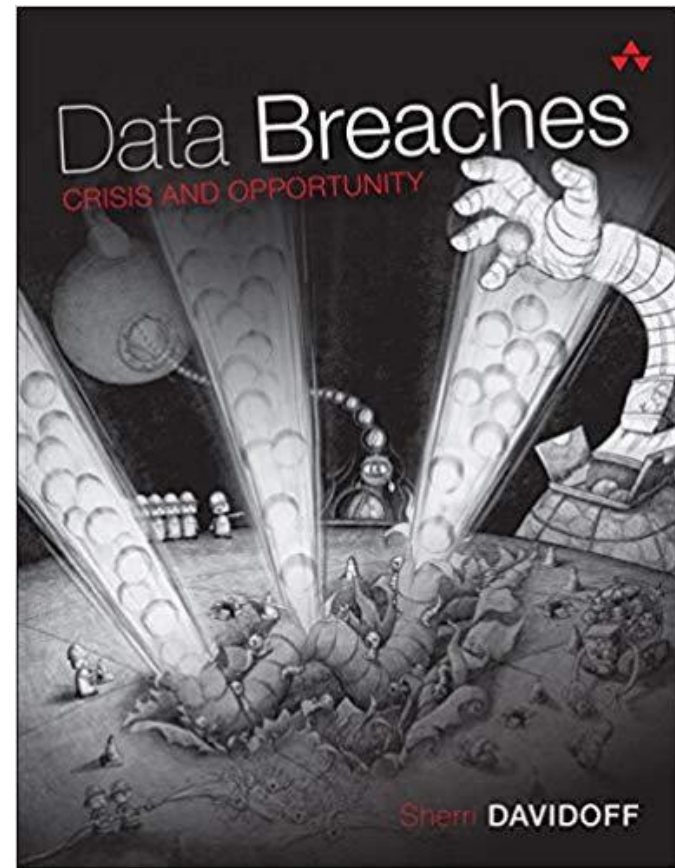
## For Employees

- ✓ Know your org's BYOD policies
- ✓ Put a strong/PIN passcode on devices
- ✓ Don't share devices
  - ✓ If you must, make a separate account
- ✓ Lock your screen
- ✓ Install antivirus and keep it up-to-date
- ✓ Use only approved file-sharing
- ✓ Don't download sensitive data w/o permission
- ✓ Try not to print sensitive data
- ✓ Don't download/install high-risk applications or engage in risky web surfing
- ✓ Report lost/stolen devices immediately



# Questions?

- Sherri Davidoff
- Email: [info@LMGsecurity.com](mailto:info@LMGsecurity.com)
  - Phone: 406-830-3165
-  @sherridavidoff
- Find me on **LinkedIn**



# Note

## **Disclaimer**

The descriptions contained in this communication are for preliminary informational purposes only and should not be taken as legal advice. The product is available on an admitted basis in some but not all US jurisdictions through Beazley Insurance Company, Inc., and is available on a surplus lines basis through licensed surplus lines brokers underwritten by Beazley syndicates at Lloyd's. The exact coverage afforded by the product described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk. Beazley USA Services, Inc. is licensed and regulated by insurance regulatory authorities in the respective states of the US and transacts business in the State of California as Beazley Insurance Services (License#: 0G55497). BZEM089\_US\_04/20.

