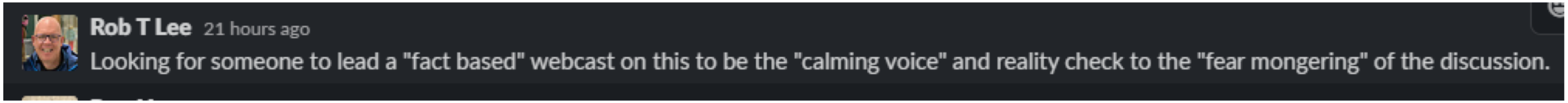
SANS

ZOMG it's ZOOM!!

Why this presentation?



I (Mick Douglas) was asked to do this since I had sent a few balanced Zoom tweets.

My tweets were in related to a great thread by Dave Kennedy.
(Link to his tweet thread in notes below)

Bottom line:

- There have been *serious* issues with Zoom.
- They're getting better rapidly.
- It's not all rosy, it's not all doom and gloom.

Disclaimers

Mick does not own Zoom stock…

Or any stock in any other video conferencing software.

SANS typically uses GoToWebinar for all webinars.

This time we're using Zoom to prove our point.

Agenda

ZOMG it's ZOOM

1. **Is Zoom secure?**
2. **What you can do**
3. **What is Zoom doing?**
4. **Take away resources**

Agenda

ZOMG it's ZOOM

1. **Is Zoom secure?**
2. **What you can do**
3. **What is Zoom doing?**
4. **Take away resources**

Is Zoom secure?

Yes.*

* Sad news: nothing is 100% secure.

James Atkinson @jimmyjamesuk123 · 11h

does it involve deleting zoom altogether?

1 1

DFIR Jackalope

@Lynch_M0b

Replying to @jimmyjamesuk123 @SANSInstitute and 2 others

Hopefully not....if people started deleting everything on their computer with a vulnerability.....they wouldn't have a computer left 🤔

12:49 AM · Apr 4, 2020 · Twitter for Android

Should I use Zoom?

It depends…

Ask yourself… If you'd talk about it on a phone… it's *probably* OK.

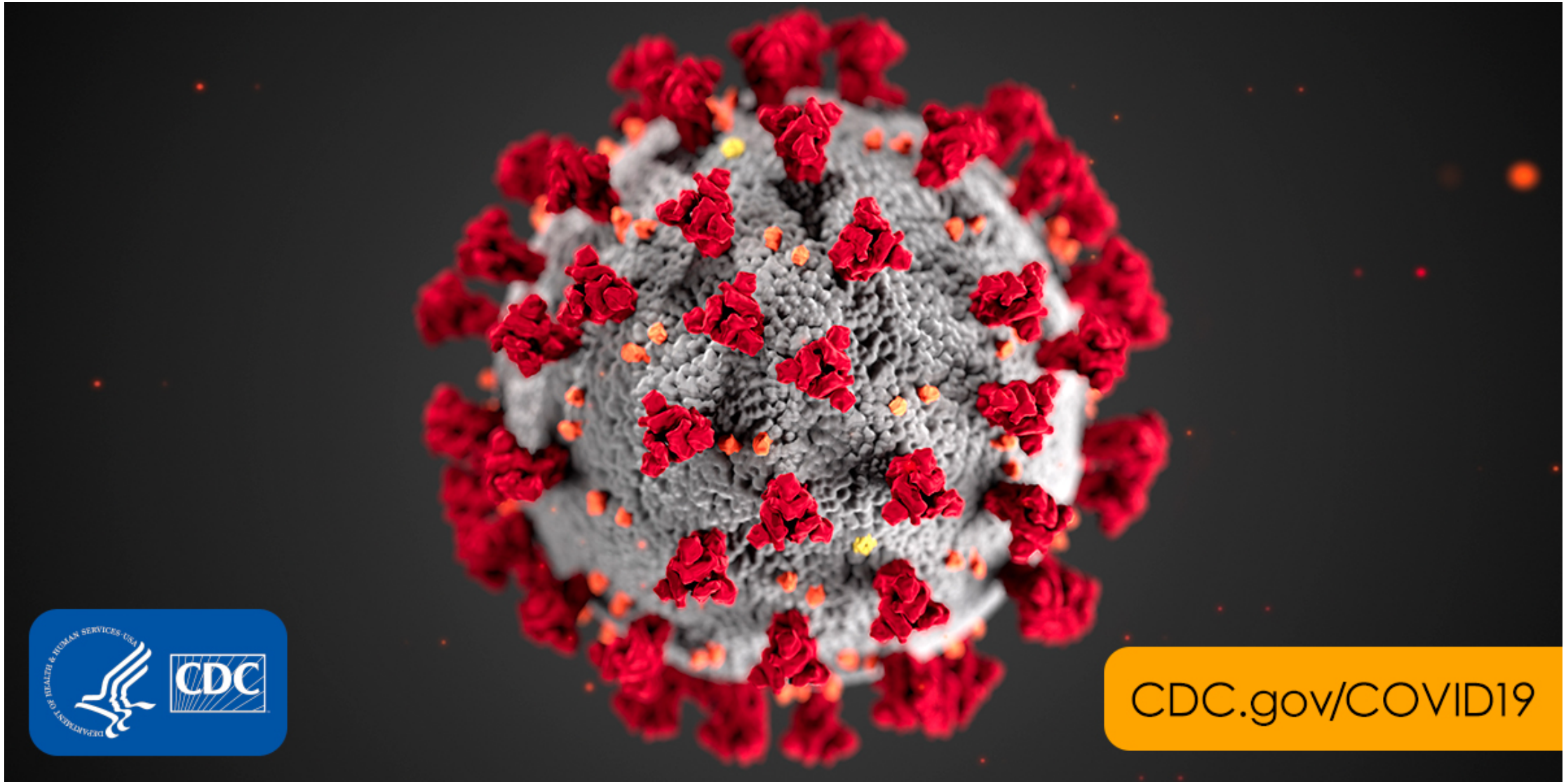
So why all the hype?

F.U.D.

Fear

Uncertainty

Doubt


DEPARTMENT OF HEALTH & HUMAN SERVICES · USA
CDC
CDC.gov/COVID19

zoom

Video Communications

Agenda

ZOMG it's ZOOM

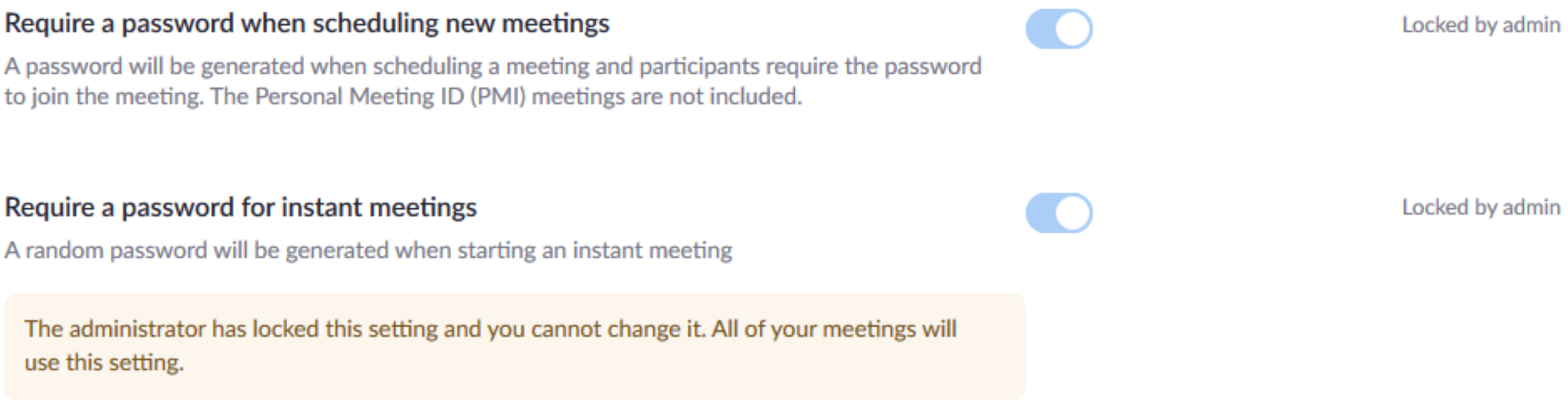
1. Is Zoom secure?
2. **What you can do**
3. What is Zoom doing?
4. Take away resources

Source: https://newsvire.com/students-are-zoom-bombing-online-classes-and-harassing-teachers-as-a-prank/

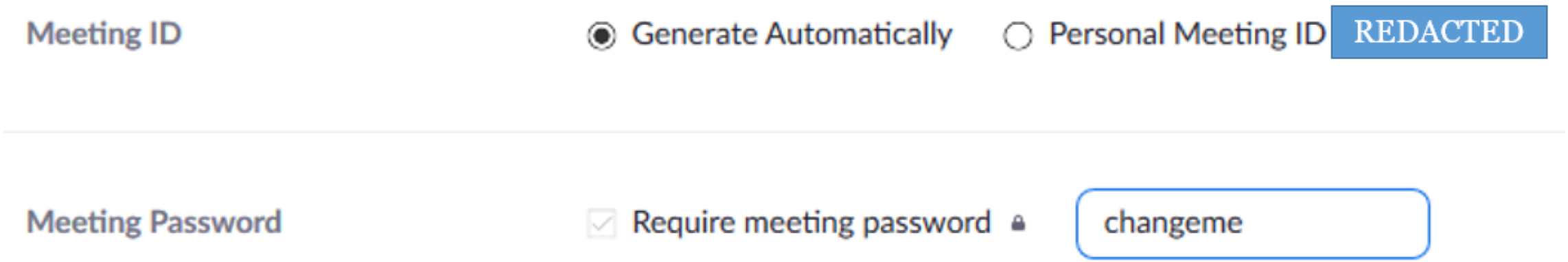
How to protect yourself

- Configure your meeting!
- Update your client.
- Be careful what you click.

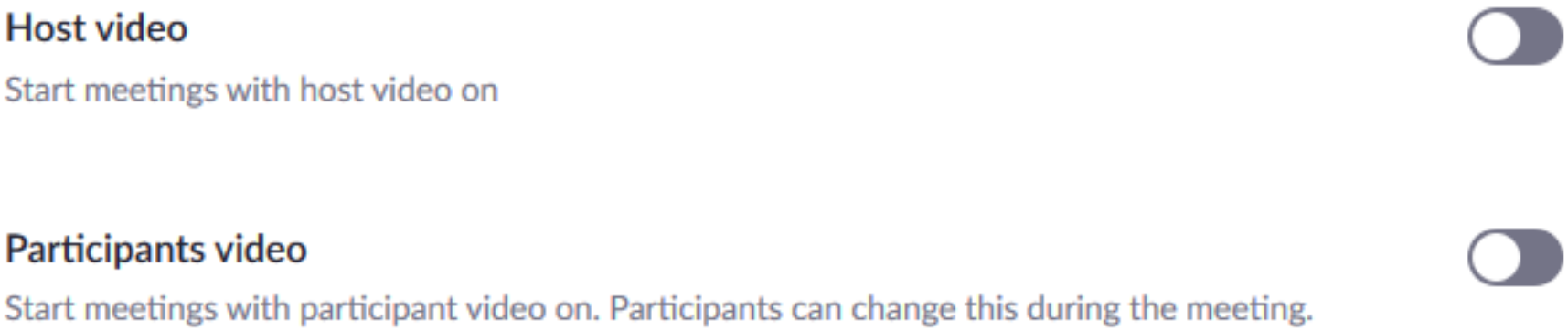
Configure your meeting: require passwords



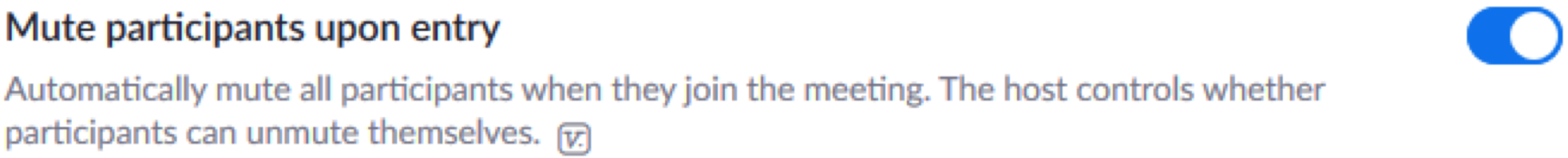
Configure your meeting: Meeting ID & passwords



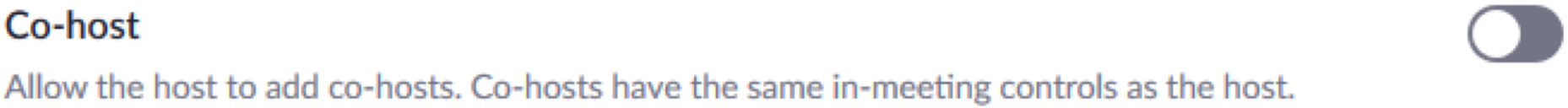
Configure your meeting: Disable video by default



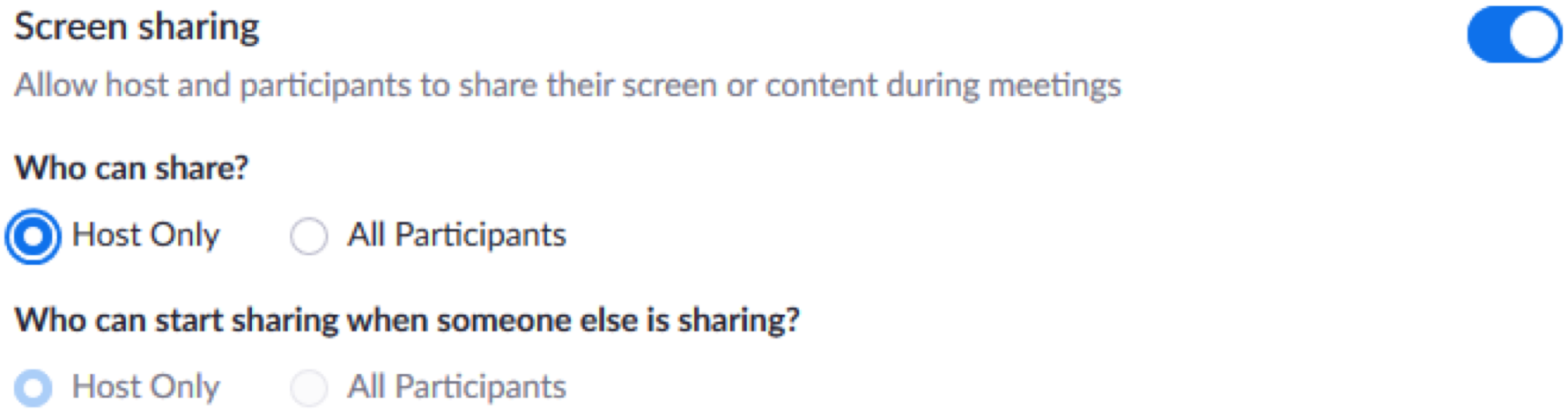
Configure your meeting: mute users by default



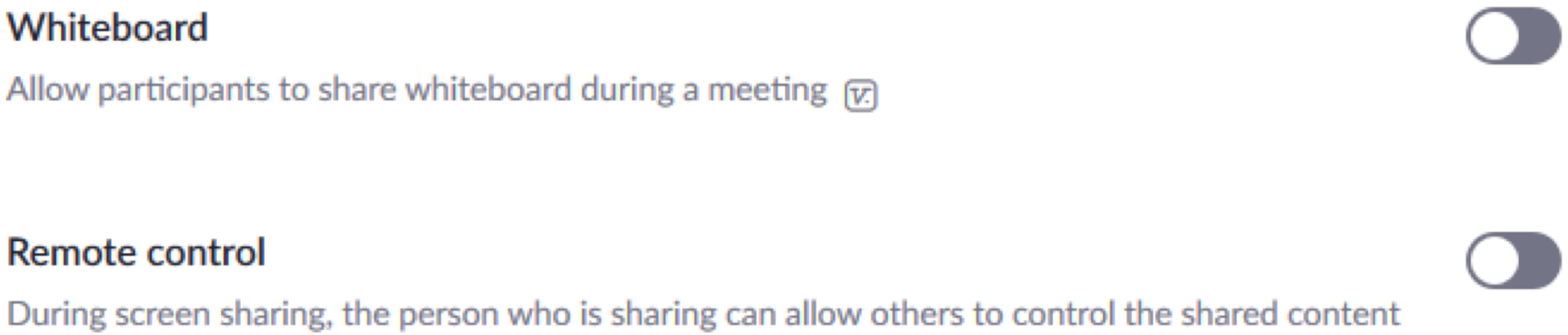
Configure your meeting: be careful of co-host!



Configure your meeting: Only allow host to screen share!!!



Configure your meeting: Don’t allow graffiti



Update Your Zoom Client

Be Careful What You Click

- Phishing invites
- Links in Zoom chat

Be Careful What You Click

Mick Douglas is inviting you to a scheduled Zoom meeting.

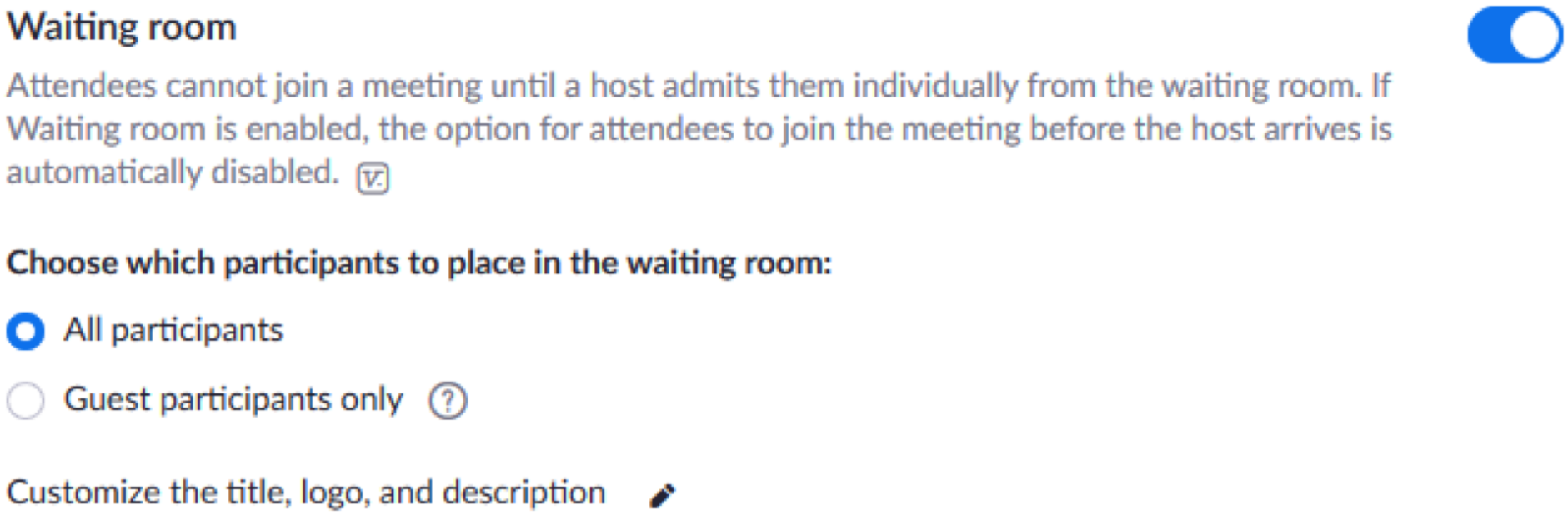
Topic: ZOMG IT'S ZOOM
Time: Apr 4, 2020 01:00 PM Eastern Time (US and Canada)

Join Zoom Meeting
https://zoom.us/j/REDACTED

Hyperlinks can point ANYWHERE!

- Only accept meetings you expect.
- Hover over link before clicking.

Configure your meeting: use the waiting room



Agenda

ZOMG it's ZOOM

1. Is Zoom secure?
2. What you can do
3. **What is Zoom doing?**
4. Take away resources

What Zoom is doing

- Fixing poor defaults
- Addressing issues researchers have discovered

Most important point:
Zoom has been transparent

Zoom scorecard as of 20200404

Issue	Grade	Reason for grade
Default passwords		Passwords are now enabled by default.
“end-to-end encryption”		Misleading use of term. Zoom is getting better quickly.
Routing meetings through China		Meetings no longer are routed through China
Waiting rooms		Not enabled by default. Apparently vulnerable.
Privacy policy		They have one… but it could be clearer.

Note: Please refer to links in notes section for references. (This deck will be available for download)

Mick's personal take: it's getting better

Many "unforced errors"

- No indicators of evil intent
- Perhaps moving a bit too fast

Agenda

ZOMG it's ZOOM

1. Is Zoom secure?
2. What you can do
3. What is Zoom doing?
4. **Take away resources**

Again, should I use Zoom?

Most likely, yes.

If you're talking about nation state "Top Secret" information on webinar software, you're doing it *WRONG*.

THANK YOU!!

- Citizen Lab
- Dave Kennedy
- Rob Lee
- SANS instructor corps!
- You!!

Get **SANS** World-Class Training On **Your Schedule Online**

OnDemand = Self-Paced training with 24/7 access to training platform and hands-on labs

Live Online = Instructor-led training offered globally in 1, 2, 3 or 6 week options in multiple time zones

Learn more at sans.org

OnDemand = Self-Paced training with 24/7 access to training platform and hands-on labs

Live Online = Instructor-led training offered globally in 1, 2, 3 or 6 week options in multiple time zones

Get **SANS** World-Class Training On **Your Schedule Online – sans.org**

SANS FREE

Resources for the Cybersecurity Community

Cybersecurity News & Alerts | Tools & Workstations | Scholarship & Community Programs | Challenges & More

sans.org/free

SANS FREE - Resources for the Cybersecurity Community

Cybersecurity News & Alerts:

- Blogs
- Newsletters: NewsBites, @Risk and OUCH!
- Internet Storm Center & ISC Podcast
- Whitepapers & Tech Talks
- Webcasts

Tools & Workstations:

- SIFT Workstation
- REMnux
- EZTools
- Slingshot
- SOF-ELK
- KAPE
- bstrings
- AmcacheParser
- EZViewer
- Jumplist Explorer

Scholarship & Community Programs:

- Cyber Discovery – UK High School
- Girls Go CyberStart – US High School
- Cyber FastTrack – Collegiate focus
- Federal Cyber Reskilling Academy
- Diversity Cyber Academy
- Women's Immersion Academy
- VetSuccess Academy
- Accelerated Cybersecurity Training Program at Ryerson University
- MD EARN Cyber Academy

SANS.org/FREE

Additional Resources:

- CyberStart Game
- CIS Critical Security Controls
- Community Night Presentations
- Cyber Aces
- Cybersecurity Posters
- Cheat Sheets
- Industry Research & Analysis
- Difference Maker Awards
- Government and Enterprise Partnerships
- GridEx 2-Day NERC Training Event
- Holiday Hack Challenge
- Missing Persons CTFs
- NetWars Cyber Range Challenges
- Annual SANS Security Awareness Report
- Security Policy Templates
- Solutions Forums
- Top 25 Software Errors
- Technology Connections Events

Resources

Download for more Zoom best practices

This presentation is available at:

https://www.sans.org/webcasts/zomg-zoom-114670

Questions?

Even though the webinar is over… the conversation is just starting!

Start chatting about this on Twitter!

#SecureZoom

Bonus Materials: Glossary and additional references

In this section we'll cover the following:

- Encryption attacks.
- Phishing.
- UNC Link Attack.
- Zoom Bomb.

And questions asked during the webinar.

Encryption Attack

Zoom has several issues to address with encryption.

Non-Technical:

- They are making confusing statements about the strength and use of the encryption.

Technical:

- The way the keys are handled leave them open to various attacks.
- Even if you do not get the key, you can “view” the video.

Phishing

Zoom is NOT at fault for the rise of Zoom based phishing attacks.

However, do to the rapid rise in using Zoom, some users are not familiar for what to look for.

UNC Link Attack

Zoom is partially at fault for this attack… It has already been fixed. This type of attack no longer works in Zoom chat.

The UNC attack is one where a web browser will send a Window's user's username and password hash to a remote system. This is by design; it is how local networks sometimes share resources. This is problematic if an attacker can launch this attack. It allows the attacker to steal the username and password hash.

Zoom Bombing

Zoom is partially at fault for this attack… They have taken steps to fix this. Please refer to the section.

Questions from the Webinar

No Zoom?

How can we stop the use of Zoom in our org?

If you don't want to have Zoom at all, you have several options:

1. Use application whitelisting to prevent the Zoom client from launching.
2. Block the IP ranges for Zoom (please see notes below)

Responsibility?

Does Zoom have a responsibility for enforcing security?

Yes. They are taking great steps. Around the time of the webinar, Zoom made passwords mandatory for ALL meetings. Based on how quickly they are responding, it is my belief that Zoom is taking their responsibility seriously and are taking the advice of the experts to heart.

VPN?

Does VPN help secure your Zoom meeting?

Not really… Zoom is hosted online and does not require VPN access to connect. The only thing a VPN does is protect attackers from stealing keys at the start of the meeting. Attackers can still do Zoom Bomb attacks by trying to brute force access to the network with tools like zWarDrive.

Citizen Lab Report?

What are your thoughts on the Citizen Lab report?

I think it's a fantastic bit of research and lovely technical writing. I also think Zoom agrees since they made a blog posting exclusively to the findings it had. One thing worth noting, Zoom has already addressed several of the findings in the report.

Marketing vs. Tech?

What are your thoughts about the differences between Zoom's marketing materials and how the product works?

In the webinar, I referred to "unforced errors"… This is exactly what I was meaning. There's no reason for such a discrepancy and as such has caused several (including the author of this webinar) to wonder why such lapses occurred. That said, Zoom is NOT alone in having issues such as these. Zoom does appear to be making the claims good or adjust the claims.

Phishing protections?

How can we protect against the increased phishing attacks using Zoom as the ruse?

Your options will be determined based on what mail infrastructure you have in place. The best thing you can do is ensure you have spam/phishing filtering capabilities that are up to date. Consider engaging the professional services of your mail filtering provider if you do not have

What do users need to know?

What training should we give users for running Zoom?

Here's a few ideas:

1. Have them use good passwords. Easily guessable ones should be avoided.
2. Use the waiting room.
3. Do not admit anyone you don't know. NEVER promote someone to co-host unless you're SURE it's the right person.

Unless otherwise credited, all photos are from pixabay
https://pixabay.com