In this issue:

Welcome to your April Cybersecurity newsletter. Cybersecurity has been in the news often this month. The primary story has been around security on the video platform Zoom. We will address some ways you can secure your Zoom account in today's newsletter as well as:

- Scams targeting your CARES Act stimulus check
- A major hotel chain breach
- Ways to secure your Nintendo Switch
- And more

Zoom Meeting Security: 5 Steps to Ensure You Don't Get Zoombombed

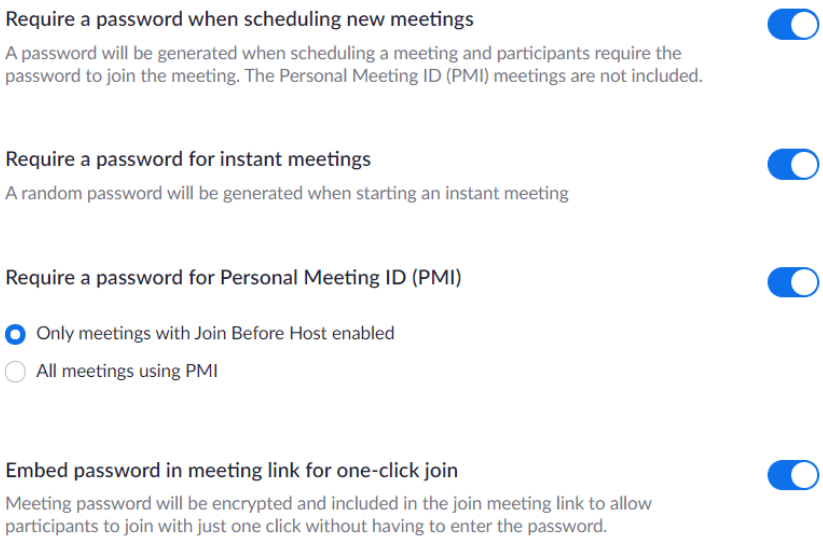
Dissertation defenses, religious services, educational workshops and more have all gone virtual as half the world's population practices social distancing. But as these events move to the popular online streaming service Zoom, hackers have taken advantage of the software's open security settings. A phenomenon now being called "Zoombombing" has unfortunately led to some online meetings being disrupted.

Zoombombing occurs when an unwanted participant joins a Zoom meeting and disrupts it with lewd, racist, or off-topic comments. These hackers have ruined important virtual events and brought some Zoom security issues to light. While the number of Zoom meetings that have been disrupted like this is small, it is important to be sure you are protecting your events in the best way possible as more client meetings and events take place online.

1. Password protect your meetings

The first action you must take to protect your Zoom meetings is to require a password for participants to use when joining. Only people who have the password will be able to join the meeting. Zoom is now making this setting the default for new accounts, but if you have an existing account, you will need to go into your settings and make the change.

To check your account, go to www.zoom.us and click "My Account." Choose "Settings" and scroll down to view the password options. Be sure to enable the items as shown in this screenshot:



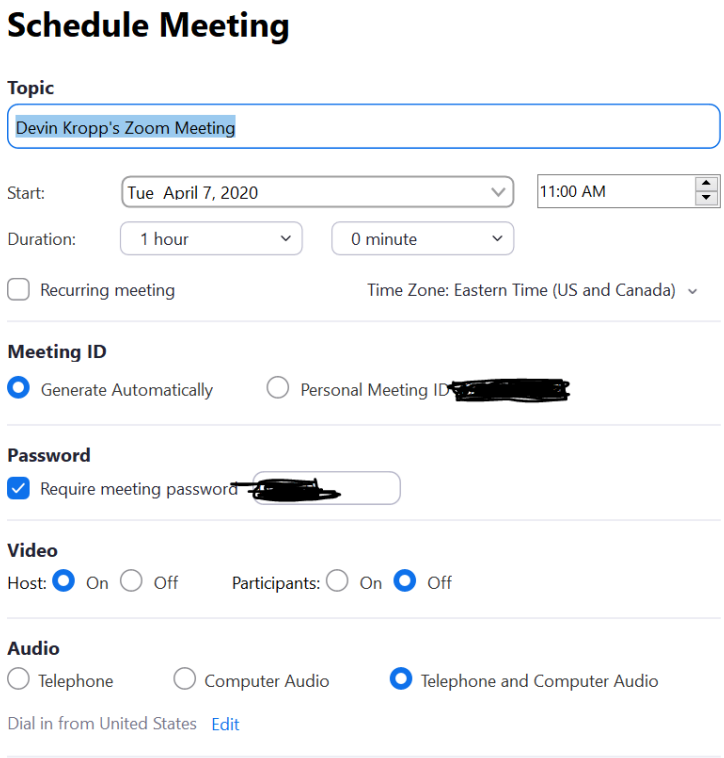
Source: Zoom

Once you have made these changes, you must be careful with your meeting passwords. Only share the password with individuals you want to join—don't post the details on social media.

2. Don't use your Personal Meeting ID

All Zoom users are issued a Personal Meeting ID (PMI) to use when scheduling a meeting. Sharing your PMI is useful for internal meetings with individuals you meet with regularly. These people will be able to use your PMI to join any future meetings you schedule with them. However, when having larger meetings with outside participants, you want to generate a one-time meeting ID.

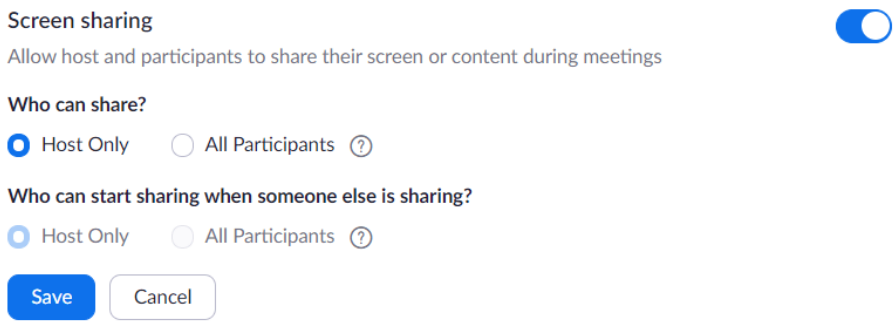
To schedule a meeting with a random PMI, open the Zoom interface on your device. Click "Schedule" and in the meeting details, choose "Generate Automatically" under Meeting ID.



Source: Zoom

3. Limit participants' sharing ability

It will be more difficult for anyone to disrupt your meeting if they cannot share their screen, video, or audio. For all meetings, only the presenter(s) should be allowed to share their screen. This will prevent participants from sharing their screen with the entire meeting. Limit screen sharing by going to www.zoom.us and viewing your Settings. Scroll down to In-Meeting Settings and select "Host Only" under "Who can share?"



Source: Zoom

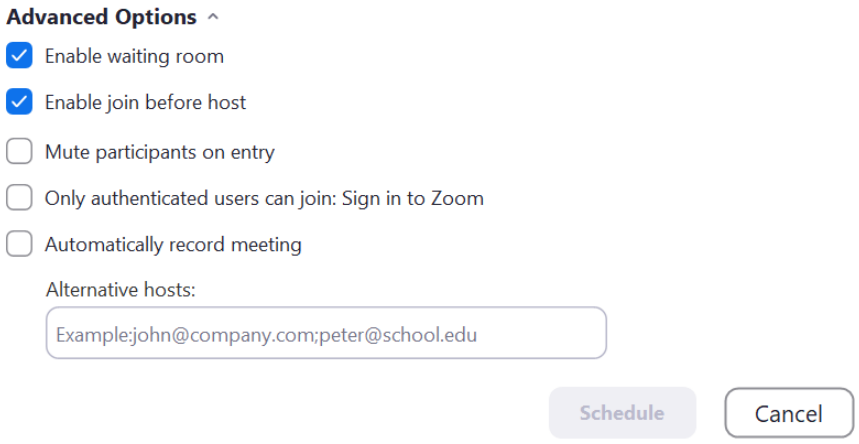
If the meeting does not require attendee participation, you should also choose to turn off video and audio sharing for all attendees. To mute all attendees, select "Manage Participants" once you have begun your meeting. There choose "Mute All" and then uncheck "Allow participants to unmute themselves."

Unfortunately, you cannot disable video for all attendees at once for Zoom meetings. However, you can individually disable this setting attendee by attendee. In “Manage Participants” you can turn off the video-sharing capability for each attendee.

4. Enable the meeting waiting room

Zoom’s waiting room feature allows the meeting host to see the attendees trying to join the meeting before the meeting starts. Enabling this feature will allow you to review attendees before the meeting and remove those you do not recognize prior to the meeting starting.

When scheduling your meeting on Zoom, select “Advanced Options” in the Schedule Meeting interface. Check the box next to “Enable Waiting Room.”



Source: Zoom

Once your meeting starts, you can lock the meeting so no other individuals can join. Go to the Manage Participants panel and click “Lock Meeting.”

5. Know how to remove participants

While taking the above steps should minimize the risk of a Zoombomber crashing your meeting, you need to know how to remove an unruly participant. This is also done in the Manage Participants panel of your meeting. Click the participant you want to kick out, select “More,” and then choose “Remove.” This will kick the attendee out of the meeting and not allow them to rejoin.

Know your options

Zoom has committed to improving security over the next 90 days. In the meantime, Zoom users must enable the security settings we outline above. Zoom’s popularity has been connected to its ease of use for participants and the overall quality of its sound and video. Of course, there are many other online meeting platforms you can use. If you are uncomfortable using Zoom, research some alternative programs to find one that better fits your needs. Options include GoToMeeting, Webex, Skype, Join.me, and Google Hangouts.

Coronavirus scams

The Federal Trade Commission is warning consumers of an increase in Coronavirus-related scams. Many of these scams are targeted at seniors, with hackers pretending to be from the Social Security Administration or Medicare. There are also scams about fake coronavirus testing kits and fake charities. Hackers perpetrate these scams via phone calls and phishing emails. Be extra careful before giving out any money or personal information. Read more about the scams here.

Beware of stimulus check fraud. The Better Business Bureau is reporting on various CARES Act check scams. In one scam, hackers call and say you are eligible for a special COVID-19 relief payment. They ask for your information to process but use that information maliciously. Another scam claims you need to pay a processing fee to get your check—you do not. The IRS will not call you about your stimulus check. If you receive a call or strange email—delete it.

Stimulus checks could be intercepted by hackers thanks to new IRS website. To get checks to Americans who do not file tax returns or don't have bank account information on file with the IRS, the agency set up a website where you can enter your bank information. The problem? Hackers could log in first and submit their bank information under your name according to security expert, Brian Krebs. While we have not seen this fraud yet, it may be wise to log in and update your bank information yourself if you have not supplied it to the IRS previously.

Unemployment benefits are being stolen by identity thieves. As millions lose their job due to COVID-19, someare in for an even biggerhit when they goto file for unemployment. Some have reported filing only to learn that someone else was already collecting benefits in their name. Others are being hit with unemployment-related phishing emails where thieves try to collect personal information in order to file for benefits under the victim's name.

Cybersecurity shorts

Marriot suffers data breach affecting over 5 million customers. The hotel chain announced the incident this month, stating that hackers got into the system through two employee's compromised credentials. Marriot guests may have had their names, birthdays, emails, phone numbers and Marriott account numbers exposed. The hotel chain will contact those who are affected.

Nintendo Switch users: Enable two-factor authentication now. Nintendo Switch sales have skyrocketed recently, but so have security concerns. Hackers have begun targeting Switch users—many have reported unauthorized access to their account. To keep your device secure, be sure to enable two-factor authentication. You can see the steps to do so here.

New report finds that advisors are at a greater risk of work-at-home phishing messages. According to RightSize Solutions, there has been an increase in phishing messages appearing to be from clients to financial advisors. The most common messages request a fraudulent wire transfer. Experts say advisors must take precautions while working from home—FINRA has not made allowances for advisors working remotely. Now is a good time to review your cybersecurity firm policies.

Small businesses applying for Coronavirus-related Economic Injury Disaster Loan may have had personal information exposed. The Small Business Association released a statement saying that a limited number of businesses may have had information exposed to other business applicants. The SBA is notifying affected businesses.

IRS warns tax professionals of an influx in tax scams as the tax season has been extended until July 15. There has been an influx in phishing emails targeted at tax professionals regarding tax deadline changes or appearing to come from clients. The IRS is encouraging tax professionals to be on the lookout for these fraudulent messages. The agency has updated its Security Summit program to reflect these new scams.

Software updates

Apple: iPhone users are at risk of a zero-day flaw. Security firm, ZecOps discovered a set of malicious emails that were sent to iPhone users beginning in 2018. Viewing these emails can cause phones to crash. Apple has created a fix in its next update, iOS 13.4.5 which is currently in beta. Be sure to upload your iPhone as soon as you are notified of a software update.

Microsoft: This month Microsoft has released updates for over 100 security vulnerabilities in its programs. About 20 of these flaws are considered critical and some are being exploited so users should update now. Affected programs include Windows 7 and 10 operating systems and Internet Explorer. Your device should prompt you to update automatically but you can read more about the updates here.

Microsoft released a second update a few days again for a zero-day exploit. The flaw impacts Microsoft Office 2019 and Microsoft Office 365 users, as well as various Windows 10 programs. Your device should prompt you to update and you can read more about the vulnerability here.

Oracle: Oracle released an update for its problematic program, Java, this month. This update closes 400 security issues. Java is a notoriously buggy program, and if you do not need it—you should delete it. Read more about the update here.