OUCH! August 2020

SANS SECURITY AWARENESS

Virtual Conferencing Safely and Securely

What is Virtual Conferencing?

With so many of us now working from home, you are most likely finding yourself remotely connecting with your co-workers using virtual conferencing solutions like Zoom, Slack, or Microsoft Teams. Your family members - perhaps even your children – may also be using these same technologies to connect with friends or for remote learning. Regardless of why you are connecting, here are key steps you can take to make the most of these technologies safely and securely.

Attending a Virtual Conference

If you will be attending a virtual conference, here are five key steps.

1. **Update the Software**: Make sure you are always using the latest version of the conferencing software. The more recent and updated your software, the more secure you will be. Enable automatic updating and quit your program when done, so it can check for the latest updates the next time you restart.
2. **Configure Audio / Video Settings**: Set your preferences to mute your microphone and turn off your video when joining a meeting and enable them only when you want. Consider placing a webcam cover or tape over your computer's camera to ensure privacy when you're not actively broadcasting. Remember: if your camera is on, everyone can see what you are doing even when you are not talking.
3. **Double-Check What's Behind You**: If you want to enable your webcam, be aware of what's behind you. Ensure you do not have any personal or sensitive information visible behind you during a call. Some video conferencing software lets you blur or use a virtual background, so people cannot see what is behind you.
4. **Don't Share Your Invite**: The invite link is your personal ticket to enter the meeting. Even if a trusted co-worker needs the link, it's much better they ask the conference organizer for their own invite.
5. **Do Not Record**: Do not take screenshots of or record the conference call without permission. You could accidentally share very sensitive information if those screenshots or recordings become public.

Hosting a Virtual Conference

If you will be hosting a virtual conference, here are some additional steps you should take.

1. **Require a Password**: To protect the privacy and security of your conference and control who can join, protect your meeting with a password. This way only people who have the conference password can join the event.
2. **Review Attendees**: Review the people attending your event. If there is someone you do not know or cannot identify, have that person confirm their identity. If you have any concerns, or if someone is being rude or disruptive, remove them from the conference. Many solutions offer the option to lock the conference once it has begun, so no one else can join unless you let them in. Another option may be to initially place people in a virtual waiting room, so you can approve who joins the call.
3. **Inform if Recording**: If you intend to record the event (and have permission to record), be sure to inform everyone on the conference ahead of time.
4. **Sharing Your Screen**: If you will be sharing your computer screen at any point, be sure to first close all other applications and remove any sensitive files from your computer's desktop. Also disable any pop-up notifications. This helps ensure you don't accidently share sensitive or embarrassing information while sharing your computer screen. Another option is to consider sharing just the program you want to show instead of sharing your entire computer screen.

These technologies are a fantastic tool and, in many ways, represent the future of how we will work, collaborate, and communicate with others. These simple steps will go a long way to ensure you safely and securely make the most of them.

Guest Editor

Lodrina Cherne is the Principal Security Advocate at Cybereason, protecting all people and information in today's open and connected world. She also teaches Windows forensics at the SANS Institute and contributes to the blog ThisWeekin4n6. Follow her on Twitter at @hexplates.

Resources

Passwords: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Password Managers: https://www.sans.org/security-awareness-training/resources/password-managers-0

Translated for the Community by:

OUCH! Is published by SANS Security Awareness and is distributed under the Creative Commons BY-NC-ND 4.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify it. Editorial Board: Walter Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley