ISSUE: May YEAR: 2021

Security Awareness Newsletter

Preparing people to lead extraordinary lives

Technology is a useful servant but a dangerous master.— Christian Lous Lange

6 Zoom Tips to Make Your Meetings More Secure

1. Send out Meeting Invites

One good practice to implement is to send attendees meeting invites. You can do this through Microsoft Outlook. This will give you more control over who can attend your meeting or webinar. In Microsoft Outlook, attendees can RSVP so you'll have a heads up of who's planning to attend.

2. Enable the Waiting Room Feature

By turning on the Waiting Room feature, you'll be able to control who enters your meeting. You'll be able to see who is waiting to join and can admit them or remove them. If you don't recognize the individual trying to join the meeting, you can remove them, and this will prevent them from joining back in.

Here's how to enable the Waiting Room feature:

- Go to "Account Management" > "Account Settings"
- Under "Security" if the Waiting Room feature is disabled, you toggle it on
- If you want to make this required for everyone on the Zoom account, click the lock to make it mandatory.

3. Require a Passcode

A good way to prevent unwelcome guests from joining your Zoom meeting is to require participants to enter a passcode before logging onto the meeting. For instance, if someone outside of your organization or group gains access to the Zoom meeting link you've generated, and a passcode is not required, they could potentially access confidential information. Passcodes prevent such intrusions.

Here's how to require a passcode:

- Go to "Account Management" > "Account Settings"
- Under "Security" you can toggle on the passcode feature if it's not already enabled
- You can also lock this feature so that a passcode will be required for all of your account users whenever they set up a meeting or webinar

4. Once Everyone's There, Lock the Meeting

Before you start the meeting, check to see if everyone's there, and lock the meeting to prevent anyone else from joining in. This is another helpful way to prevent "Zoom Bombing" so they'll be no surprise guests.

Here's how to lock your Zoom meeting:

- Look down the bottom of the Zoom meeting window and click "Participants"
- From here, you'll see a button that says "Lock Meeting" that you can select

5. Use a Generated Meeting ID, Not Your Personal One

Never use your personal meeting ID for group settings, such as a team meeting or classroom setting. If someone you're not familiar with obtains your personal meeting ID, they'll be able to join your meeting space and may do so unannounced. It's best to use generated Zoom IDs, such as by scheduling a meeting.

Here's how to schedule a Zoom meeting with a generated ID:

- You can create a Zoom meeting through the online Zoom app or the desktop client.
- Online, under the "Meetings" tab, you can click the "Schedule a New Meeting" button to begin setup.
- On your desktop, go to the Zoom client and click "Schedule."
- From here, you can fill in the details of the meeting and opt to have an ID generated by making sure the radio button is selected under "Meeting ID"

6. Manager Who Can Share Their Screen

Prevent unexpected distractions or screen sharing by managing who can share during a meeting, training session, lecture, or even social gathering. This way you can keep everyone focused and centered.

Here's how to manage who can share their screen in Zoom:

- In your host controls next to the "Share Screen" option, click on the arrow
- Next, click "Advanced Sharing Options"
- Under the "Who can share?" option, select "Only Host"

What is Data Loss Prevention?

What is Data Loss Prevention?

Data loss prevention (DLP) makes sure that users do not send sensitive or critical information outside the corporate network. The term describes software products that help a network administrator control the data that users can transfer.

DLP products use business rules to classify and protect confidential and critical information so that unauthorized users cannot accidentally or maliciously share data, which would put the organization at risk. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission.

Organizations are adopting DLP because of insider threats and rigorous data privacy laws, many of which have stringent data protection or data access requirements. In addition to monitoring and controlling endpoint activities, some DLP tools can also be used to filter data streams on the corporate network and protect data in motion.

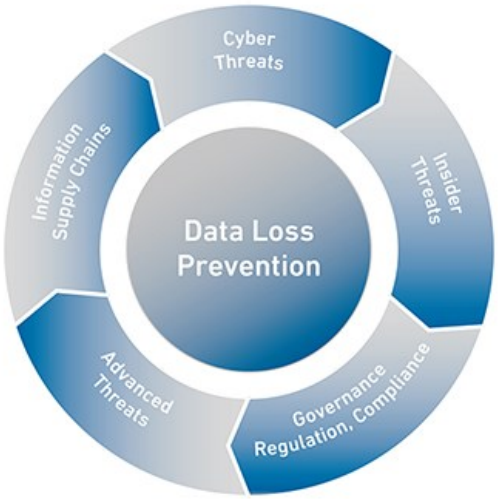
Organizations typically use DLP to:

- Protect Personally Identifiable Information (PII) and comply with relevant regulations
- Protect Intellectual Property critical for the organization
- Achieve data visibility in large organizations
- Secure mobile workforce and enforce security in Bring Your Own Device (BYOD) environments
- Secure data on remote cloud systems

Causes of Data Leaks

Three common causes of data leaks are:

Insider threats — a malicious insider, or an attacker who has compromised a privileged user account, abuses their permissions and attempts to move data outside the organization.



Extrusion by attackers — many cyber attacks have sensitive data as their target. Attackers penetrate the security perimeter using techniques like phishing, malware or code injection, and gain access to sensitive data.

Unintentional or negligent data exposure — many data leaks occur as a result of employees who lose sensitive data in public, provide open Internet access to data, or fail to restrict access per organizational policies.

For more information on DLP, visit our website https://www.luc.edu/its/services/datalossprevention/

2021 Cybersecurity Trends to Watch For

- On average, only 5% of companies' folders are properly protected.
- Data breaches exposed 36 billion records in the first half of 2020.
- 45% of breaches featured hacking, 17% involved malware and 22% involved phishing.
- 94% of malware is delivered by email.
- Since the pandemic began, the FBI reported a 300% increase in reported cybercrimes.
- Remote workers have caused a security breach in 20% of organizations.

University Information Security Office
LUC.edu/its/uiso/

ITS Service Desk
Email: ITSservicedesk@luc.edu
Telephone: (773) 508-4487
Hours: LUC.edu/its/service/support_hours.shtml