Kính gửi: BGH các trường TH, THCS trong huyện.

Căn cứ các công văn chỉ đạo của Sở GD Hà Nội và Phòng GD Gia Lâm về việc triển khai dạy học qua internet, tính đến thời điểm hiện tại 100% các trường đã triển khai dạy học qua internet tới học sinh, đa số các nhà trường triển khai dạy học qua phần mềm Zoom Meeting. Phần mềm Zoom Meeting bước đầu cho thấy hiệu quả của việc sử dụng, giáo viên và học sinh dễ dàng cài đặt và đăng nhập, song thực tế đã xảy ra lỗ hỏng về mặt bảo mật trong các giờ dạy của các buổi học trực tuyến dẫn đến các đối tượng xấu đã lợi dụng lỗ hỏng bảo mật đó đăng nhập vào giờ học của giáo viên và học sinh tung tin và một số hình ảnh, video không lành mạnh ảnh hưởng đến kết quả giờ học và tâm lý của học sinh, giáo viên. Trước tình hình thực thế như vậy, Phòng GDĐT đề nghị các nhà trường thực hiện một số nội dung sau:

1/ Các nhà trường chủ động thực hiện các giải pháp để bảo mật thông tin giờ học khi triển khai dạy học qua internet bằng các phần mềm ( Zoom, O365...)

2/ Khuyến khích các nhà trường chủ động liên hệ các nhà cung cấp hỗ trợ miễn phí dạy học trên internet trong đợt dịch Covid theo công văn 968/SGDĐT-GDPT ngày 27 tháng 3 năm 2020 về việc hỗ trợ dạy học trực tuyến trong các trường phổ thông để được tư vấn và cung cấp phần mềm có bản quyển hỗ trợ trong dạy học ( Các trường nghiên cứu và chọn đơn vị cung cấp cho phù hợp).

3/ Quản lý tài khoản của giáo viên và học sinh khi đăng nhập các phần mềm dạy học trực tuyến như lập danh sách số điện thoại hoặc email đăng ký tài khoản Zoom hoặc các tài khoản khác của Giáo viên và học sinh; Yêu cầu ghi rõ họ và tên giáo viên; họ và tên học sinh,lớp,trường khi đăng nhập để dễ quản lý.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Gợi ý cách sử dụng Zoom an toàn, tránh rò rỉ thông tin cá nhân**

Trước tình hình dịch [Covid-19](https://thanhnien.vn/tin-tuc/covid-19.html) đang diễn ra phức tạp, thay vì hoạt động ở văn phòng, trụ sở, các công ty đang có xu hướng khuyến khích nhân viên làm việc từ xa.

Chính vì vậy, các nền tảng truyền thông trực tuyến đã trở thành công cụ thiết yếu cho cá nhân và doanh nghiệp tương tác trao đổi công việc. Với thị phần toàn cầu chiếm gần 20% và hơn 12,92 triệu người dùng hoạt động hằng tháng, [Zoom](https://thanhnien.vn/cong-nghe/zoom-go-bo-phan-gui-du-lieu-nguoi-dung-toi-facebook-1202942.html) trở thành một trong những nền tảng giao tiếp phổ biến nhất được sử dụng để tổ chức hội thảo, các cuộc họp ảo, đào tạo... trực tuyến. Điều này dẫn tới nguy cơ nền tảng này đang trở thành mục tiêu hấp dẫn cho các tin tặc.

Theo báo cáo của Check Point Research - tổ chức cung cấp thông tin về các mối đe dọa không gian mạng, vừa qua đã xảy ra các cuộc tấn công từ bên ngoài để nghe lén các cuộc họp, các cuộc trò chuyện riêng tư... được thực hiện thông qua ứng dụng Zoom, từ đó có khả năng dẫn đến vi phạm dữ liệu cá nhân hoặc gián điệp [kinh doanh](https://thanhnien.vn/tai-chinh-kinh-doanh/).

Vậy làm thế nào có thể tận hưởng những tiện ích của [Zoom](https://thanhnien.vn/tin-tuc/zoom.html) mà không khiến bản thân trở thành con mồi của các cuộc tấn công mạng? Dưới đây là một số lời khuyên từ các chuyên gia đến từ Công ty cổ phần An ninh mạng Việt Nam VSEC.

**1. Luôn cập nhật phiên bản mới nhất**

|  |
| --- |
| Để duy trì bảo mật hiệu quả, phần mềm Zoom phải được cập nhật thường xuyên. Các bản cập nhật không chỉ bổ sung các tùy chọn và [tính năng mới](https://thanhnien.vn/cong-nghe/kinh-nghiem/) mà còn sửa lỗi cũng như vá các lỗ hổng bảo mật được tìm thấy từ các phiên bản trước - chẳng hạn như khả năng thực hiện nghe lén các cuộc họp đã đề cập ở trên.Cách sử dụng Zoom an toàn, tránh rò rỉ thông tin cá nhân - ảnh 1  Ảnh chụp màn hình |

Cần phải lưu ý rằng, cơ hội để tin tặc tấn công không chấm dứt khi các lỗ hổng đã được vá, bởi những người dùng chưa cập nhật bản mới vẫn tồn tại các lỗ hổng này. Chỉ khi người dùng cập nhật phần mềm và nhận bản vá của Zoom thì các mối đe dọa ở bản cũ mới có thể được giải quyết.

**2. Sử dụng mật khẩu trong các cuộc họp**

Các chuyên gia VSEC cho biết, với mỗi cuộc hội thảo thì Zoom sẽ tạo ra một ID gồm 9-11 ký tự là các số ngẫu nhiên. Với hình thức tấn công brute force - kỹ thuật để thử các kết quả có thể có để dò tìm ID meeting, các tin tặc có thể đánh cắp các ID một cách dễ dàng và xâm nhập vào hội thảo mà người host không hề biết. Việc tấn công này xảy ra trong trường hợp hội thảo không cài đặt mật khẩu.

|  |
| --- |
| Cách sử dụng Zoom an toàn, tránh rò rỉ thông tin cá nhân - ảnh 2  Ảnh chụp màn hình |

Để tránh các sự cố ở trên, Zoom cung cấp lựa chọn tạo mật khẩu cho cuộc họp. Như vậy khi người lạ có biết ID của cuộc họp thì còn cần phải có mật khẩu trước khi tham gia vào cuộc .

**3. Sử dụng tính năng “Waiting room”**

Để bảo đảm các cuộc họp của người dùng chỉ bao gồm những người tham gia mà host mong muốn. Zoom bổ trợ tính năng kiểm soát người tham gia cuộc họp - waiting room. Sau khi kích hoạt tính năng này, mỗi khi có một người mới tham gia sẽ ở trong trạng thái chờ để host xét duyệt quyền tham dự cuộc họp.

|  |
| --- |
| Cách sử dụng Zoom an toàn, tránh rò rỉ thông tin cá nhân - ảnh 3  Ảnh chụp màn hình |

**4. Quản lý chia sẻ màn hình**

Để cung cấp cho host nhiều quyền kiểm soát hơn cũng như ngăn chặn người tham gia chia sẻ màn hình với các nội dung không mong muốn. Zoom đã cung cấp tính năng “Only Host” trong tab “Advanced Sharing Options” tức là chỉ có host là người duy nhất có thể chia sẻ nội dung trong cuộc họp.

Ngoài một số mẹo sử dụng Zoom an toàn nói trên, các chuyên gia VSEC cũng khuyến cáo người dùng cần nâng cao nhận thức trước các hình thức tấn công Phishing.

|  |
| --- |
| Cách sử dụng Zoom an toàn, tránh rò rỉ thông tin cá nhân - ảnh 4  Ảnh chụp màn hình |

Nếu bạn sử dụng Zoom lần đầu tiên, hãy đảm bảo bạn đang tải xuống trực tiếp từ trang *zoom.us* chứ không phải bất kỳ domain nào khác (z00m.us...). Ngoài ra, người dùng không tải xuống trình cài đặt phần mềm Zoom thông qua mạng chia sẻ ngang hàng (BitTorrent, eMule, Gnutella...) hay từ những địa chỉ trang web trung gian.