

OUCH!

نشرة الوعي الأمني الإخبارية الشهرية للجميع

عقد المؤتمرات الافتراضية بأمان

ما هي المؤتمرات الافتراضية؟

نظرًا لأن الكثير منا يعمل الآن من المنزل، فمن المرجح أن تجد نفسك على اتصال عن بُعد مع زملائك في العمل باستخدام حلول المؤتمرات الافتراضية مثل Zoom أو Slack أو Microsoft Teams. قد يستخدم أفراد عائلتك وربما حتى أطفالك هذه التقنيات نفسها للتواصل مع الأصدقاء أو للتعلم عن بُعد. بغض النظر عن سبب اتصالك، إليك الخطوات الرئيسية التي يمكنك اتخاذها لتحقيق أقصى استفادة من هذه التقنيات بأمان.

حضور مؤتمر افتراضي

إذا كنت ستحضر مؤتمرًا افتراضيًا، فإليك خمس خطوات رئيسية لزيادة درجة الأمان:

1. تحديث البرنامج : تأكد من أنك تستخدم دائمًا أحدث إصدار من برنامج المؤتمرات الافتراضية. كلما كان برنامجك حديثًا ومحدثًا، ستكون أكثر أمانًا. قم بتمكين التحديث التلقائي، وإغلاق البرنامج الخاص بك عند الانتهاء.
2. تكوين إعدادات الصوت / الفيديو: اضبط صوت الميكروفون والفيديو عند الانضمام إلى اجتماع في وضعية التعطيل (الإيقاف أو الكتم) وتمكينها فقط عندما تريد. ضع في اعتبارك وضع غطاء على كاميرا ويب أو شريط فوق كاميرا الكمبيوتر لضمان الخصوصية عندما لا تقوم بنشاط. تذكر: إذا كانت الكاميرا قيد التشغيل، يمكن للجميع رؤية ما تفعله حتى عندما لا تتحدث.
3. تحقق مرة أخرى مما وراءك: إذا كنت تريد تمكين كاميرا الويب الخاصة بك، فكن على دراية بما هو خلفك. تأكد من عدم وجود أي معلومات شخصية أو حساسة مرئية خلفك أثناء المكالمات. يتيح لك بعض برامج مؤتمرات الفيديو تعقيم أو استخدام خلفية افتراضية، حتى لا يتمكن الأشخاص من رؤية ما وراءك.
4. لا تشارك دعوتك: رابط الدعوة هو تذكرك الشخصية لدخول الاجتماع. حتى إذا كان زميل عمل موثوق به بحاجة إلى الرابط، فمن الأفضل أن يطلب دعوتك الخاصة من منظم المؤتمر.
5. عدم التسجيل: لا تأخذ لقطات شاشة أو تسجل المكالمات الجماعية بدون إذن. يمكنك عن طريق الخطأ مشاركة معلومات حساسة للغاية إذا تم مشاركة هذه التسجيلات للعامة.

استضافة مؤتمر افتراضي

إذا كنت ستستضيف مؤتمرًا افتراضيًا، فإليك بعض الخطوات الإضافية التي يجب عليك اتخاذها:

1. طلب كلمة مرور: لحماية خصوصية وأمان المؤتمر والتحكم في من يمكنه الانضمام، قم بحماية اجتماعك بكلمة مرور. بهذه الطريقة فقط الأشخاص الذين لديهم كلمة مرور المؤتمر يمكنهم الانضمام إلى الحدث.
2. مراجعة الحضور: راجع الأشخاص الذين يحضرون الحدث الخاص بك. إذا كان هناك شخص لا تعرفه أو لا يمكنك تحديده، اطلب منه تأكيد هويته. إذا كان لديك أي مخاوف، أو إذا كان شخص ما غير مهذب أو مزعج، فقم بإزالته من المؤتمر. تقدم العديد من الحلول خيار قفل المؤتمر بمجرد أن يبدأ، لذلك لا يمكن لأي شخص آخر الانضمام إلا إذا سمحت لهم بالدخول. قد يكون الخيار الآخر هو وضع الأشخاص في البداية في غرفة انتظار افتراضية، بحيث يمكنك الموافقة على من ينضم إلى المكالمات.
3. التبليغ عند التسجيل: إذا كنت تنوي تسجيل الحدث (ولديك إذن بالتسجيل)، فتأكد من إبلاغ الجميع في المؤتمر مسبقًا.
4. مشاركة شاشتك: إذا كنت ستشارك شاشة الكمبيوتر في أي وقت، فتأكد أولاً من إغلاق جميع التطبيقات الأخرى وإزالة أي ملفات حساسة من سطح مكتب الكمبيوتر. قم أيضًا بتعطيل أي إشعارات منبثقة. يساعد هذا على ضمان عدم مشاركة معلومات حساسة عن طريق الخطأ أو معلومات محرجة أثناء مشاركة شاشة الكمبيوتر. خيار آخر هو النظر في مشاركة البرنامج الذي تريد عرضه فقط بدلاً من مشاركة شاشة الكمبيوتر بالكامل.

هذه التقنيات هي أداة رائعة، في شتى المجالات. فهي تمثل كيفية العمل والتعاون والتواصل مع الآخرين في المستقبل. ستقطع هذه الخطوات البسيطة شوطًا طويلاً لضمان تحقيق أقصى استفادة منها بشكل آمن.

المحرّر الضيف

Lodrina Cherne لودرينا شيرن هي المسؤولة الأمنية الرئيسية في [Cybereason](#)، تقوم بحماية الأشخاص والمعلومات، كما تقوم بتدريس [الطب الشرعي لنظام تشغيل Windows](#) في معهد SANS وتساهم في المدونة [ThisWeekin4n6](#). يمكنكم متابعتها على تويتر [على hexplates@](#).



الموارد

أنشئ كلمات مرور سهلة: <https://www.sans.org/security-awareness-training/resources/making-passwords-simple>

برامج إدارة كلمة المرور: <https://www.sans.org/security-awareness-training/resources/password-managers-0>

ترجمها للعربية: محمد سرور، فؤاد ابو عويمر، درويش الحلو، اسلام الكرد
OUCH! تُنشر! من قبل فريق الوعي الأمني في SANS وتُوزع بموجب [الرخصة Creative Commons BY-NC-ND 4.0](#). لك الحرية في المشاركة أو توزيع هذه النشرة الإخبارية شرط عدم تعديلها أو بيعها. الفريق التحريري: والت سكريفنس، فل هوفمان، ألان واغونر، شيرلي كونلي