Northbridge Insurance

RISK INSIGHTS

CYBER SPIES: HOW TO SAFELY USE WEBCAMS AND VIDEO CONFERENCING

When teams work remotely, they often prefer to use video conferencing for meetings. Webcams enable richer communication where participants can pick up visual cues in addition to verbal conversation. From a cybersecurity standpoint, you need to choose the right video conferencing service and use best practices to protect your computer system and files.

THESE SIX TIPS WILL HELP YOU SELECT A SAFE VIDEO CONFERENCING PLATFORM AND SECURE YOUR WEBCAM:

"Free" is not usually free

If you are not paying for a product or service, it is safe to assume that you are the product. In other words, free services usually collect information about you that they can monetize. They also may not invest as much in security. Choose a paid web conferencing solution instead.

Restrict meeting access

You need to have tight control over who is in the meeting. Choose a conferencing solution that allows you to issue a different PIN code for each meeting and restricts access to attendees who can enter the code. Your conferencing platform should identify each person in attendance by name and/or email address/phone number. You don't want a hacker spoofing the identity of a colleague or coworker, so choose a platform that makes it difficult to conceal or change your identifications details. Ask all attendees to announce themselves at the start of the meeting.

Insist on end-to-end encryption

Public and shared Wi-Fi access can leave user data vulnerable to man-in-the-middle attacks. Video conferencing for work will often involve discussions of sensitive business information, so only consider web conferencing solutions that offer end-to-end encryption. That provides an extra layer of security that makes conferences and communication harder to intercept.

Look around your office

How much personal information could be gleaned about you by the items in your office? Do you have photos with your spouse and children? College diplomas or certifications on the wall? Bank statements or passwords on your desk? A video conferencing platform with a virtual background or greenscreen can help conceal your personal environment.

Secure your webcam

When not properly secured, webcams can offer an intimate and deeply personal level of intrusion to would-be hackers. Change and update the default administrator login and password from the manufacturer. Keep the webcam software up-to-date with the latest security patches and updates. If you use an external webcam, turn it off and cover it when not in use to prevent cyber spying. For an internal webcam, such as in a laptop, you can affix a Post-It note over the camera lens.

Consider a firewall

Hackers discover and access webcams by probing networks for unsecured points of entry. Setting up a firewall or configuring your Internet router to block unwanted incoming Internet traffic can add another level of protection for your webcam, computers, and other devices on your home network.

For more information on making your business safer, contact our Risk Services Department at **1.833.692.4111** or visit us at **www.nbins.com**.

[3889-001-ed03E | 05.2020]

CYBERSCOUT®