keeping your event data secure

Best Practices for Digital Safety

Corporate marketers often lull themselves into a false sense of security – and thus vulnerability – by assuming, "Our event is too small," or "Our industry is too niche."

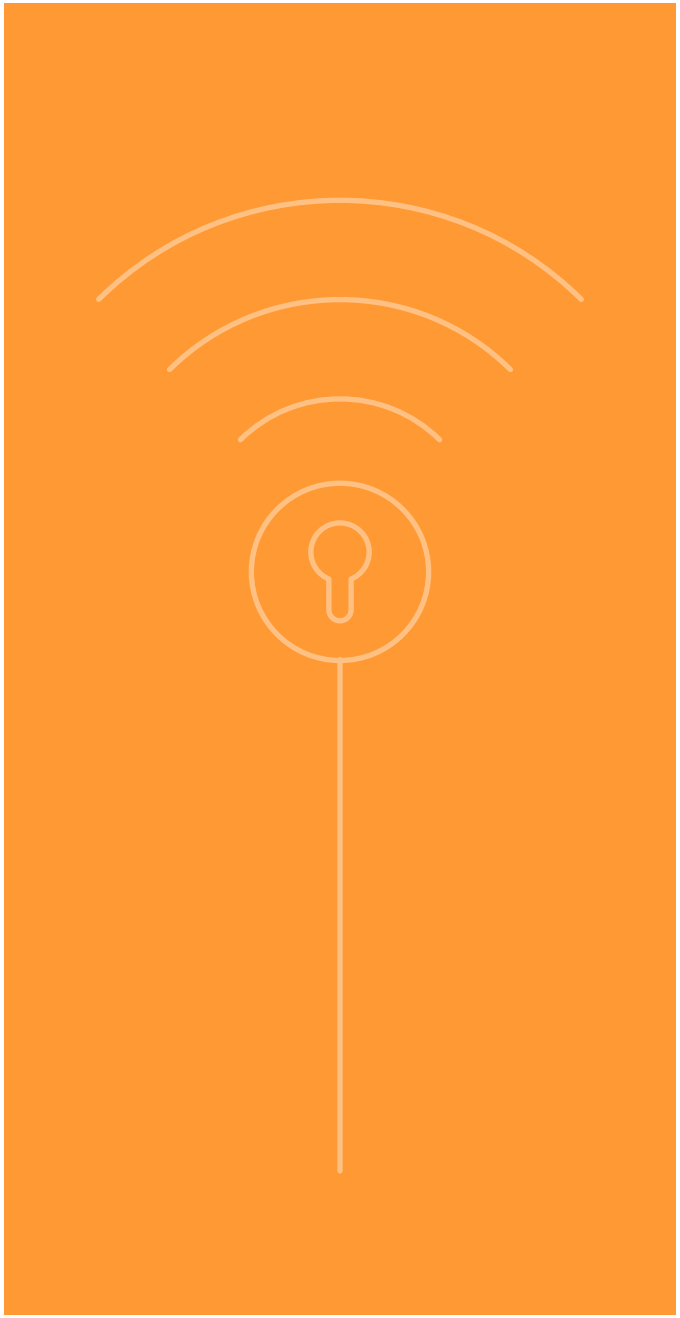
But the Internet is crawling with hackers' automated software looking for any and every opportunity. A registrant's credit card info is just as valuable if she's attending a 100-person conference as a 10,000-person event. Many events also include confidential information about strategies and forthcoming products, such as in NDA-only presentations to analysts and investors.

A cautionary example came out of the 2016 Republican National Convention: in a single day, more than 1,200 attendees connected to fake Wi-Fi hotspots around the Quicken Loans Arena and at Cleveland Hopkins International Airport. With legitimate-sounding names such as "Google Starbucks" and "Attwifi," the hotspots exposed user information, such as identities, emails, and the websites they visited.

The good news is that the hotspots were part of a test by Avant Software,[1] which makes mobile and PC security products. The bad news is that hackers frequently use these and other tactics to target events of every type.

Mitigating cybersecurity risks and vulnerabilities can seem daunting, but it is more important than ever in the age of always-on, always-available technology. Understanding why Wi-Fi enables so many types of hacks, for example, is critical to guiding the implementation of simple pre-event IT best practices that can help protect laptops and other devices your employees travel with. And while it's true that the event environment can create unique security and privacy challenges, by considering event IT security as an extension of office security policies, you have a natural starting point.

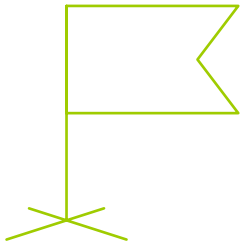
Mitigating cybersecurity risks and vulnerabilities can seem daunting, but it is more important than ever in the age of always-on, always-available technology.



[1] Avast Software: Amidst Charged Cyber Security Dialogue, Republican National Convention Attendees Show Negligent Behavior http://www.businesswire.com/news/home/20160719006378/en/Avast-Software%C2%A0Amidst-Charged-Cyber-Security-Dialogue-Republican

hope for the best, plan for the worst

There are several reasons why hackers frequently target trade shows, conventions, product launches, and other events:



Event staff, attendees, exhibitors, and presenters are in an unfamiliar place, and may not be as familiar with or aware of red flags. They know the name of their office Wi-Fi network. At the event venue, however, their device will provide several to choose from. As the Avant Software test demonstrated, a Wi-Fi hotspot name that sounds legitimate may actually belong to a hacker who wants to collect passwords, credit card numbers, and other confidential information.

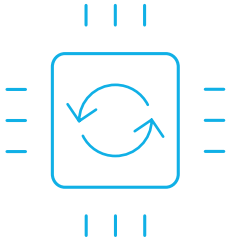
Event strategies and product demos frequently include proprietary or confidential information, including details about company strategies and forthcoming products. A sneak peek could enable a hacker to gain access to product plans and specs that would open the door for copies to flood the market, for example.

The event venue's Wi-Fi network is often overloaded. Hundreds or thousands of people trying to connect simultaneously has always been a challenge for even the best-engineered Wi-Fi networks. Now there are additional challenges, such as the increased bandwidth required by HD videos that attendees, exhibitors, and presenters increasingly stream, upload, and download. All of this adds up to slow connections, which often prompts employees to use their smartphone to create a hotspot. Unless they use a virtual private network (VPN) to secure those connections, those personal hotspots are vulnerable.

Hundreds or thousands of people trying to connect simultaneously has always been a challenge for even the best-engineered Wi-Fi networks.

extend office security policies and best practices to events

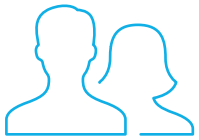
Many IT security policies and best practices used in the office and for non-event travel are highly effective at events too. Here are four to consider:



Make sure all laptops, smartphones, Wi-Fi routers, and other devices that employees take to the venue are up to date with security patches before they go. In 2015, the 10 most common hacks exploited vulnerabilities that were more than a year old, and 68 percent of those were at least three years old, according to Hewlett Packard Enterprise's 2016 Cyber Risk Report.[2] A major reason these weaknesses become easy targets is because IT departments have so much on their plate that patches get pushed to the back burner.

[2] Hewlett Packard Enterprise 2016 Cyber Risk Report, http://hpe.com/software/cyberrisk

Some organizations make patch projects manageable by focusing on the most vulnerable systems rather than everything at once. The laptops and other devices that employees take to events should be atop the priority list.



Remind staff of relevant travel policies. Many security best practices for other types of travel, such as sales calls, apply to events too. Two examples are making sure their smartphones' hotspot capability is turned off, and using a VPN when connected to a public hotspot.

Many businesses contract with Wi-Fi providers such as Boingo and iPass because it's cheaper than having employees choose and expense hotspots on their own. Those services typically come with software that automatically connects to their hotspots, eliminating the risk of using a hacker's. Some also include VPNs in their software.

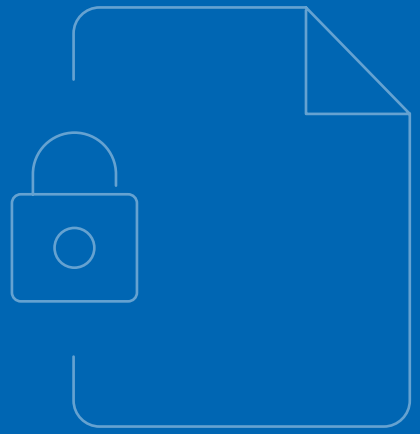
Make it a policy that employees must connect to official networks only.
If your organization is hosting the event, consider using event signage and event portals to educate attendees, presenters, and exhibitors about security in printed materials, as well as in the app's event information. Let attendees know through the mobile app which network is the official one. Provide the password only in secure places, such as parts of the venue that require an attendee badge. Displaying it in the show floor guide or on digital signage in the lobbies makes it accessible to anyone off the street — including potential hackers.

Secure the office. Hackers often target laptops and other portable devices not just for the information that's on them, but also because they provide a back door to network-based resources. Make sure the office IT infrastructure has firewalls, intrusion protection systems (IPS), and other safeguards to block unauthorized traffic coming from laptops, servers, and other devices that employees take to events.

Educate employees about the importance of extending office policies and best practices to the event environment. One example is using a VPN for sensitive information, such as downloading a confidential presentation from the cloud. If your organization is hosting the event, provide the same advice to exhibitors.

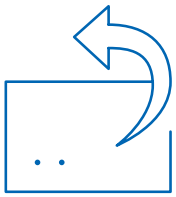
Don't let your guard down outside the venue. Hackers can target devices just about anywhere, especially during an event. Make sure employees follow policies and best practices throughout their trip: at the airport, the hotel, cafés, and anyplace else where they connect over Wi-Fi.

create a privacy policy



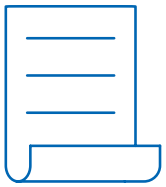
Although businesses typically have IT privacy policies for their offices, they often don't create one when hosting events.

That's a mistake because it's the foundation for protecting employees, customers, business partners, and others they interact with at the event. Here are several tips to consider when developing a privacy policy:



Remember that with control comes responsibility. If data will be shared — such as attendee info with exhibitors — make it clear who owns the data and what can be done with it.

Display the privacy policy prominently and include it in communications with exhibitors and attendees. For example, if the event provides Wi-Fi, put it on the page that users see when they connect. Another place is the registration website. If the event has a mobile app, make reading and accepting the policy a condition for using the app.



Spell out the details. In the policy, explain the types of information collected, what will be done with it, and whether/how it will be shared with third parties. Look for opportunities to explain how attendees benefit from allowing their information to be collected. For example, tracking session attendance helps the event's host identify popular topics and presenters. The policy should acknowledge that usage, but emphasize that attendees will also be offered access to online archives of related sessions they didn't attend.

Make it clear who owns the data and what can be done with it.

bring in the experts

Some events offer a mobile app to engage attendees in ways such as helping them find session rooms and interact with presenters.

Event hosts often hire third parties to develop those apps because they don't have that expertise on staff. When it comes to maximizing security/privacy, outsourcing has its benefits and risks.

The experts know more about the technology because they work with it on a daily basis. This experience means they'll know more about its vulnerabilities than an IT generalist. Their expertise is particularly valuable when implementing new technologies, such as near-field communications (NFC) or any service that could direct your device to a location on the web, like beacons. These could enable new attack methods.

Make sure the mobile developer turns off unnecessary logging features, such as for the user's location, before shipping the app. A recent Hewlett Packard Enterprise study[3] found this is a common practice that creates major vulnerabilities.

Consider hiring an auditing/testing firm to verify that app developers, cloud providers, and other third parties are meeting security/privacy policies. PwC and Veracode are two examples.

Consider hiring a consultant with event expertise to identify potential security and privacy risks, as well as options for minimizing them. Like app developers, these firms have specialized experience that most businesses lack. At the 2012 Olympics, hackers distributed malware-infested schedules, a tactic that could be thwarted by educating attendees on how the app is the only approved way to get schedules and other official information.

[3] Hewlett Packard Enterprise Mobile Application Security Report, http://www8.hp.com/us/en/software-solutions/mobile-app-security/

stay vigilant

Whether your company is attending or hosting an event, cybersecurity should be a top priority. It's a mistake to assume that your company, event, or industry is too small or too niche to be a target. Even information as basic as names, addresses, and phone numbers can be attractive to hackers who want to steal identities and launch social engineering attacks.

To minimize vulnerabilities, start by extending existing security and privacy policies and best practices to the event environment. Next, focus on vulnerabilities that are unique to events. Hire consultants and other experts if your IT organization lacks the resources to identify and address those vulnerabilities. Together, these strategies will provide multiple layers of protection for your employees and events.