Catch the Beat not the Breach

How to Protect Yourself from a Data Breach at Your Next Concert

Office of Information Technology
Division of Information Security
JULY 2024

Summer concerts are a great way to start the season, providing amazing experiences full of music, friends, and fun. While summer concerts are exciting, they are also a prime target for cybercriminals since the large gatherings and high volume of online transactions provide a perfect opportunity to exploit concertgoers. Cybercriminals steal personal and financial information by exploiting vulnerabilities in ticket sales, public Wi-Fi networks, and social media platforms. Phishing schemes, fake ticket websites, and virus attacks are frequent methods of deceiving concertgoers. Due to the rise of digital ticket sales and cashless transactions, data breaches have increased, costing unsuspecting concert fans thousands of dollars. Here is what you need to know about how data breaches occur, their consequences, and how to protect yourself while enjoying your favorite concert.

Data breaches around concerts occur through several clever techniques. Cybercriminals may create fake ticketing websites or send phishing emails that mimic legitimate vendors, tricking concertgoers into providing personal and financial information. Concert venues often offer free Wi-Fi to attendees, but these networks are usually unsecured, allowing hackers to intercept data transmitted over free Wi-Fi connections.

Cybercriminals send fraudulent emails, texts, or QR codes that look like they come from legitimate ticket vendors or concert organizers. These messages may appear harmless but may contain malware. After clicking the link, attendees risk having malware installed on their devices or having their personal information stolen. Mobile POS (Point of Sale) systems used for concert merchandise and food purchases are another target cybercriminals use. If the network is not secure, cybercriminals can steal credit card information. Lastly, cybercriminals frequently use social engineering techniques to obtain private information from social media platforms to guess passwords or provide answers to security challenge questions.

Ticketmaster/ Live Nation (a major ticket-selling company) recently revealed that a data breach compromised thousands of customers' personal information. According to Ticketmaster, this data breach was linked to a third-party data service provider. The database contained the personal information of their customers who purchased tickets to events in North America (U.S., Canada and/or Mexico). Ticketmaster is currently in the process of contacting all of the affected customers. Along with collaborating with banks, credit card companies, and law enforcement, Ticketmaster is providing a complementary 12-month identity monitoring service to all affected customers.

You can find out more information here Ticketmaster Data Security Incident – Ticketmaster Help.

A data breach for an upcoming summer concert could have serious consequences. Victims may suffer financial losses due to stolen credit card information and identity theft. The emotional distress from privacy invasion and the hassle of dealing with the aftermath adds to such stress. Concert organizers and vendors face reputational damage, loss of customer trust, and potential legal consequences. Regulatory bodies are increasingly imposing hefty fines on organizations that fail to protect consumer data properly. If you find yourself involved in a data breach, it is critical to take immediate action to mitigate the damage.

Here are a few steps that can help:

Confirm the Breach
The first step is to confirm whether your data has been compromised. Check for official notifications from the company involved in the breach. These notifications are typically sent via email, or posted on the company's website.

Change Your Passwords
Immediately change the passwords for all affected accounts. Use strong, unique passwords for each account. Consider using a password manager to generate and store complex passwords securely. Enable two-factor authentication (2FA) wherever possible for an added layer of security.

Secure Your Devices
Keep your devices updated with the latest security patches and antivirus software, scan for malware regularly, and avoid using public Wi-Fi for sensitive transactions unless using a secure virtual private network (VPN).

Monitor Your Accounts and Review Account Security Questions
Regularly check your financial accounts for unfamiliar or unauthorized transactions, and report any suspicious activity to your bank. Change the security questions and answers for online accounts. Choose questions and answers that are not easy to guess, and are not publicly available.

Set Up Fraud Alerts
Place a fraud alert on your credit report, an extra precaution step designed to notify you before any new account is opened in your name. You can set up a fraud alert by contacting one of the three major credit bureaus: Equifax, Experian, or TransUnion.

Report Identity Theft and Consider Identity Theft Protection Services
If you notice any signs of identity theft, report it immediately to the Federal Trade Commission (FTC) through their identity theft website (identitytheft.gov). The FTC will develop a recovery plan for you based on the information you provide. Also, many identity theft protection services can monitor your personal information and alert you to potential threats. These services can also assist in identity recovery if you become a victim of identity theft.

Freeze Your Credit
A credit freeze restricts access to your credit report, making it more difficult for cybercriminals to create new accounts in your name. You can temporarily remove the freeze if you need to apply for credit. To place a freeze on your credit, contact each bureau separately.

Stay Informed
Stay up to date on the latest security practices and data breach news. Knowledge is the best defense against potential future breaches.

Additional things to be aware of around summer concerts

Fake Ticket Sales:
Cybercriminals set up fake websites, and online ads, or stand near the event venue to sell counterfeit tickets. These often look very convincing and can fool even the most cautious buyer. Purchase tickets only from trusted and official sources. Avoid clicking on links from unsolicited emails or messages, and double-check URLs to ensure you are on the correct website.

Use Secure Payment Methods:
When purchasing tickets online, choose a secure payment method such as a credit card or a reputable payment system that offers fraud protection. Avoid using debit cards, which are directly linked to your bank account.

Be Cautious of Social Media:
Always be careful when posting your concert plans on social media. Avoid posting photos of tickets with barcodes or other personal information, as cybercriminals search for such information.

Summer concerts should be a time for fun and entertainment, not worrying about potential data breaches. Involvement in a data breach can be stressful and overwhelming, but taking immediate and informed actions can significantly reduce the risk of identity theft and financial loss. **By following these steps, you can protect your personal information and ensure your digital security.**

Be safe and have an amazing summer!

NOTE: *The links in this document are for informational purposes only and do not signify an endorsement of any products contained within the linked sites/files.*

Please contact cybersecurity@ihs.gov with any questions or comments about this newsletter.