KEEPER | Pressemitteilung

# Keeper Security warnt vor den größten Cyber-Bedrohungen während der Olympischen Spiele 2024 in Paris

**MÜNCHEN, 5. Juni 2024 –** Die Olympischen Sommerspiele 2024 stehen vor der Tür, und während Millionen von Fans auf der ganzen Welt planen, das internationale Sportereignis zu verfolgen oder daran teilzunehmen, bereiten sich die Organisatoren auf noch nie dagewesene Herausforderungen im Bereich der Cybersicherheit vor. Die Olympischen Spiele, die in Paris ausgetragen werden und sich auf 16 weitere Städte in Frankreich verteilen, stellen für Athleten, Organisatoren und Zuschauer ein erhebliches Cyber-Sicherheitsrisiko dar - sowohl virtuell als auch vor Ort. Einem aktuellen Bericht von Microsoft zufolge bieten hochkarätige Sportereignisse wie die Olympischen Spiele aufgrund der vernetzten Umgebungen und der zunehmenden digitalen Transaktionen hervorragende Möglichkeiten für Cyberangriffe, was zu einem erhöhten Cyberrisiko führt.

In den letzten Jahren gab es einen deutlichen Anstieg an ausgeklügelten Cyberangriffen auf große Sportereignisse - so auch im letzten Monat, als das X-Konto der französischen Sportministerin Amélie Oudéa-Castéra gehackt wurde. Das Zusammentreffen großer Menschenmengen, umfangreicher Medienberichterstattung und kritischer Infrastruktur stellt ein attraktives Ziel für Bedrohungsakteure dar, die versuchen, den Betrieb zu stören, sensible Daten zu stehlen oder allgemein ein großes Chaos zu verursachen. Diese Bedrohungen beschränken sich nicht nur auf diejenigen, die persönlich an den Spielen teilnehmen. Hochkarätige Veranstaltungen bieten auch grenzenlose Möglichkeiten für Betrüger, Phishing-Angriffe gegen ahnungslose Opfer zu starten, die sich für die Veranstaltung interessieren.

Unabhängig davon, ob man an den Olympischen Spielen teilnimmt oder sie von zu Hause aus verfolgen will - Keeper Security hat die Cybersecurity-Bedrohungen identifiziert, auf die man achten sollte, und gibt Ratschläge, wie man sich und seine digitalen Ressourcen schützen kann.

> **#1 Vorsicht vor Phishing-Betrug**. Cyberkriminelle nutzen seit langem Phishing-Betrügereien, um persönliche Daten über E-Mails oder Textnachrichten mit bösartigen Links oder Anhängen zu stehlen. Während der Olympischen Spiele können diese Betrügereien den Anschein erwecken, von offiziellen olympischen Organisationen, Sponsoren oder seriösen Nachrichtenquellen zu stammen. Die Empfänger werden mit Versprechungen von exklusivem Zugang zu Eintrittskarten, kostenlosen Live-Streams, Preisgewinnen oder dringenden Kontobestätigungen gelockt. Die Links führen jedoch zu gefälschten Websites, die darauf ausgelegt sind, persönliche und finanzielle Informationen zu stehlen, oder sie können einen Anhang enthalten, der Malware auf das Gerät des Benutzers herunterlädt.

Mit immer ausgefeilteren Technologien, einschließlich des zunehmenden Einsatzes von KI, sind Cyberkriminelle in der Lage, immer glaubwürdigere Kampagnen zu entwickeln, um ahnungslose Nutzer zu ködern. Um zu vermeiden, Opfer eines Phishing-Angriffs zu werden, gelten nach wie vor die gleichen bewährten Praktiken für die Cybersicherheit. Öffnen Sie keine Anhänge und klicken Sie nicht auf Links aus unbekannten Quellen. Überprüfen Sie die Quelle, die Informationen von Ihnen anfordert, und kontrollieren Sie alle Links, die Sie erhalten. Betrüger nutzen auch Social Engineering, um Benutzer zu manipulieren, indem sie grundlegende Informationen online finden, um den Anschein der Echtheit zu erwecken und Menschen dazu zu bringen, ihnen Geld zu schicken oder vertrauliche Informationen preiszugeben. Halten Sie Ausschau nach Betrügern, die versuchen, sich als Freunde oder Familienmitglieder auszugeben, die dringend Geld benötigen, um Eintrittskarten zu kaufen oder auf Spiele zu wetten.

**#2 Schützen Sie alle Ihre Konten.** Wenn Sie Konten zum Streamen von Spielen, zum Verfolgen von Nachrichten oder zum Platzieren von Wetten einrichten, kann es verlockend sein, Passwörter zu verwenden, die leicht zu merken sind. Vergewissern Sie sich, dass Sie für alle Ihre Konten eindeutige, hochsichere Passwörter verwenden. Wenn ein Konto geknackt wird, kann ein Cyberkrimineller nicht auf die anderen Konten zugreifen. Passwörter sollten mindestens 16 Zeichen lang sein und eine Mischung aus Groß- und Kleinbuchstaben, eine Reihe von Sonderzeichen und eine zufällige Auswahl von Zahlen enthalten. Vermeiden Sie leicht zu erratende Informationen wie Haustiernamen, Geburtsdaten und Adressen. Ein Passwort-Manager ist von unschätzbarem Wert für die Erstellung und Speicherung sicherer Passwörter. Die Einführung einer Multi-Faktor-Authentifizierung für Ihre Konten bietet eine zusätzliche Sicherheitsebene, die vor den meisten Sicherheitsverletzungen schützt.

**#3 Überlegen Sie sich zweimal, bevor Sie kostenlos streamen.** Fans, die die Spiele verfolgen wollen, wenden sich auf der Suche nach kostenlosen Streams oft an das Internet - was häufig zu Sicherheitseinbußen führt. Es gibt zwar legitime Websites und Apps, die die Olympischen Spiele kostenlos streamen, aber es gibt auch Websites, die illegale Streams anbieten. Sie können Werbung für fragwürdige Inhalte enthalten und bösartige Links, die Malware auf Ihrem Gerät installieren könnten.

**#4 Achten Sie auf gefälschte Eintrittskarten.** Fans, die die Spiele besuchen möchten, müssen sich vor gefälschten Tickets in Acht nehmen. Betrüger erstellen überzeugende Websites, um offizielle Ticketverkaufsplattformen zu imitieren, und bieten Plätze an, die entweder gar nicht existieren oder weit überteuert sind. Kaufen Sie Tickets nur bei seriösen Anbietern, die ein sicheres Zahlungssystem und einen Regressanspruch anbieten, falls die Tickets nicht zustande kommen. Die Olympischen Spiele sind auch eine Zeit, in der mehr Fans versuchen, bei den Spielen Geld zu gewinnen, und Betrüger sind bereit, dies auszunutzen. Sie locken mit großen Preisen, aber sobald sie die Teilnahmegebühr oder die persönlichen Daten eingesammelt haben, verschwinden sie und es kommt die Gewinner erhalten nie ihre Auszahlung.

**#5 Vermeiden Sie öffentliche WiFi- und Ladestationen**. Ein öffentliches WLAN ist ein wichtiges Schlachtfeld für Cyberkriminelle und sollte niemals zum Senden persönlicher, finanzieller oder anderer sensibler Daten verwendet werden. Eine der bekanntesten Cyber-Bedrohungen im Zusammenhang mit öffentlichem WiFi ist der MITM-Angriff (Man-in-the-Middle). Da sich jeder in ein öffentliches WiFi-Netzwerk einwählen kann, haben Sie keine Ahnung, wer Ihre Online-Daten beobachtet oder abfängt. Fans sollten auch öffentliche USB-Ladestationen meiden. Cyberkriminelle können Malware auf diese Ladestationen laden, um böswillig auf Ihr Gerät zuzugreifen.

Cyberkriminelle suchen immer nach neuen und kreativen Wegen, um ihre Opfer ins Visier zu nehmen, vor allem bei hochkarätigen Sportveranstaltungen wie den Olympischen Spielen. Wenn Sie sich gegen diese Bedrohungen wappnen und bewährte Verfahren der Cybersicherheit befolgen, ist die Wahrscheinlichkeit, Opfer von Cyberkriminalität werden, deutlich geringer.

###

**Über Keeper Security:**
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die erschwinglichen und benutzerfreundlichen Lösungen von Keeper basieren auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer auf jedem Gerät zu schützen. Unsere Privileged-Access-Management-Lösung der nächsten Generation ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in jede Technologieumgebung integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern sowie Tausenden von Unternehmen und ist der führende Anbieter von erstklassigem Passwort- und Passkey-Management, Geheimnisverwaltung, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging.

Erfahren Sie mehr unter KeeperSecurity.com
Folgen Keeper: Facebook Instagram LinkedIn X YouTube

**Pressekontakt für Keeper in DACH:**
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de