European telcos inadvertently expose sensitive customer data to excessive sharing and risk

Tala Security's analysis of the websites of Europe's top mobile providers indicates that sensitive data is at risk from over-sharing and attack—with little effective security in place to prevent it

MILPITAS, Calif. —March 30, 2021— New research released by **Tala Security** today indicates that data exposure is a significant, unaddressed problem for Europe's top mobile providers and, by extension, more than 253 million customers who sign up for their services and share sensitive personal data. At the heart of the problem: insecure website supply chains.

Tala analyzed the websites of the top Mobile Service Providers in 7 European countries:

KEY FINDINGS

- **Sensitive data is at significant risk via form data exposure** - Forms used to capture credentials, banking details, passport numbers, etc., are exposed to an average of 19 third-parties. Without control, this sensitive data is at risk. This level of exposure, combined with the high value of the data captured, make this an attractive target for Magecart attacks.
- **None of the sites had effective web security in place:** On a 100-point scale where a score of 50 indicates limited control, the average within this group was 4.5.
- **100% of the websites are vulnerable to cross-site scripting** (XSS) - The most widespread website attack, which frequently results in significant sensitive data leakage.
- **The highest number of third-party JavaScript integrations** found on a single site was 735; the average was 162.

WHY IT MATTERS

Unintentional data exposure is a significant, unaddressed risk for all of the telcos analyzed. Without controls, every piece of JavaScript code running on websites - from every vendor included in the website owner's website supply chain - can modify, steal or leak information through client-side attacks enabled by JavaScript. Telcos amongst this sample group averaged 31 third-party integrations.

"In many cases, data sharing or exposure takes place via trusted, legitimate applications on the allowlist —often without the website owners' knowledge," said Deepika Gajaria, VP of Products at Tala Security.

"While most online businesses do a great job protecting data *after* the user has entered it, few seem to be aware of data leakage as an unintended consequence of the dynamic, rich website experience telcos are known for. This has potentially far-reaching implications for user privacy and, by extension, GDPR.

Unfortunately, our analysis indicates insufficient awareness of the risk. It's time for website owners to start caring about over-sharing."

"European telcos routinely collect sensitive data like passport scans, banking details, address and employment information. When website owners fail to effectively secure data as it is entered into their websites, they're effectively leaving it hanging, an accident waiting to happen," said Gajaria.

Download the Mobile Providers in the EU Web Security Report Here:
https://hubs.ly/H0K68160

About Tala Security

Tala prevents sensitive data theft and client-side attacks like Magecart, XSS, code injections and session redirects. Our data security and privacy platform protects hundreds of millions of browser sessions every month from critical and growing threats, such as data leakage, cross-site scripting (XSS), Magecart, website supply-chain attacks, clickjacking and others. It does this by automating the deployment and dynamic adjustment of browser-native, standards-based security controls such as Content Security Policy (CSP), Subresource Integrity (SRI), HTTP Strict Transport Security (HSTS) and other web security standards. The activation of browser-native security controls provides comprehensive security without requiring any changes to the application code and with almost no impact to website performance. Tala serves large website operators in verticals such as financial services, online retail, payment processing, hi-tech, fintech and education. Learn more at www.talasecurity.io

Contact
Connect Marketing
Sherri Walkenhorst
sherriw@connectmarketing.com
(801) 373-7888