Twitter Shares Updates on Its Internal Security Efforts

Twitter provided an update on some of the behind-the-scenes work it has been doing to keep its platform secure.

Chief technology officer Parag Agrawal and data protection officer Damien Kieran said in a blog post Thursday that the social network has been strengthening the checks that team members with access to its customer data, features and proprietary tools must undergo, reducing the potential for unauthorized access.

They wrote, “We have strict principles around who is allowed access to which tools and at what time, and we require specific justifications for customer data to be accessed.”

Twitter is constantly refining its internal detection and monitoring tools, which help surface unusual behavior or unauthorized attempts to access its internal tools.

Agrawal and Kieran also pointed to the security measures the social network put in place last week for high-profile election-related accounts, including requiring stronger passwords and requiring the use of two-factor authentication.

New hires at Twitter were already required to undergo security and privacy and data protection training, and Twitter added new coursed and increased the frequency and availability of existing courses for all employees.

Agrawal and Kieran provided the example that employees with access to non-public information now have two new mandatory training sessions to complete.

The social network also enhanced training in areas including privacy by design, privacy impact assessments, secure coding and threat modeling.

Agrawal and Kieran added, “Our teams have also been investing in additional penetration testing and scenario planning to help secure Twitter from a range of possible threats, including in the context of the upcoming 2020 U.S. elections. Specifically, over a five-month period from March 1 through Aug. 1, Twitter’s cross-functional elections team conducted tabletop exercises internally on specific election scenarios. Some of the topics included: hacks and other security incidents, leaks of hacked materials, platform manipulation activity, foreign interference, coordinated online voter suppression campaigns and the post-Election Day period.”

Internally, Twitter is requiring its team to use phishing-resistant security keys when authenticating to systems around the world.

And the social network has elevated the number of privacy reviews and impact assessments it conducts, going from roughly 100 in 2018, to nearly 500 in 2019, to over 300 in the first six months of 2020.

Agrawal and Kieran wrote, “We are continuing to invest more in the teams, technology and resources to support this critical work. We also know that we can do more to make it easier for you to find and use the settings and controls we offer, so we’re working on rolling out improvements to the design and navigation of our privacy settings. You’ll see these improvements in Twitter soon.”

They concluded, “We want you to have peace of mind when you come to Twitter that the data you share with us is secure, and that you understand and feel empowered to use the controls we offer you to keep your account secure. This will always be ongoing work for us, but trust that we are committed to acting

in the interest of the people who use our service. Where we discover an issue, we will work quickly to fix it, learn from it and hold ourselves accountable by keeping you informed.”

Recommended articles
https://www.adweek.com/programmatic/twitter-shares-updates-on-its-internal-security-efforts/