Inspired eLearning March Newsletter

INSIGHTS FROM THE X-FORCE THREAT INTELLIGENCE INDEX

Read about key findings from the 2021 IBM X-Force Threat Intelligence Index as well as their predictions for 2021.

READ BLOG

PROTECTING YOUR PEOPLE FROM RANSOMWARE IN 2021

Ransomware attacks can impact more than just your organization. Learn about 2021 threats and how to protect your business.

READ BLOG

Combating Call Center Fraud in the Age of COVID

With many agents now working from home, call centers require new technology, new processes, and a new way of thinking about security.

Call centers are a fraudster's dream. Millions of pieces of personally identifiable information (PII) are transmitted from customers to service agents every day. Anyone able to infiltrate these systems — either physically or digitally — can turn around and make a small fortune selling all sorts of valuable information on the Dark Web. In fact, according to Aite Group, 61% of fraud originates in the call center.

During normal operations, security is extremely tight.

Agents are authenticated with an ID badge, their arrivals and departures are tracked, and they are not even allowed to have a pen or pencil when taking calls. But these are not normal times. COVID-19 has shifted more than 1 million agents from locked-down call centers to work-from-home systems — weakening physical security strategies meant to prevent rogue actors from exfiltrating information for personal or financial gain.

Now, more than ever, it is critical that organizations with large call center operations take advantage of new, innovative technology to secure the conversation.

Preventing Work-From-Home Security Risks

Agents working from home can't be monitored and tracked while on the job to the extent they are in the call center. For example, they can't be prevented from recording calls or writing down credit card numbers and other financial information. Organizations can't even authenticate users who log in to their call center platforms with photo IDs — meaning that a family member, a roommate, or even a stranger could impersonate the agent and harvest valuable PII.

Here are three tips that organizations can use to secure the conversation:

1. Prove Agents Are Who They Say They Are
Speech recognition and voice biometric technology in the call center are nothing new. Organizations often use these technologies to authenticate customers that call in and to evaluate intent. But speech recognition and voice biometrics can be used on the agent side as well. Agents can be verified when they first log in and then periodically throughout the entire shift. This prevents an unauthorized person from using stolen credentials or sneaking into the system when the agent is on a break. If there is an inconsistent or false match, a supervisor is notified immediately and can address the situation.

2. Automate and Encrypt PII Collection
Rogue agents and unauthorized users can't steal information they don't know. Instead of relaying PII verbally over the phone, customers can submit information digitally without any agent exposure. This can be done over text or encrypted SMS that pings a server on the back end and sends the agent a confirmation to continue the engagement once the data is accepted. An added benefit is the ability to automatically populate redundant fields across applications. Previously, an agent might have had to manually enter information multiple times across screens. Automating data collection can reduce call times by half and eliminate human error.

3. Detect Anomalies With AI
All call center calls are recorded for quality of service and security but, with thousands of calls conducted every day, not all can be monitored. Artificial intelligence (AI) and machine learning (ML) can close that gap by parsing through conversations to identify abnormal behavior at scale. These solutions can search for changes in tone, long pauses, and other indications that something unexpected has occurred. It can even learn to remove bias from fraud detection — such as forgiving specific speech patterns from agents that have a speech impediment or accent. By leveraging AI, systems are able to constantly learn and adapt models to improve accuracy.

We expect to see millions of agents handling customer service calls from the comfort of home rather than a highly secure, highly controlled call center. Securing the conversation will require organizations to investigate new technologies that can identify and prevent fraud in these situations — from speech biometrics to audio encryption to AI. Fraudsters are now on notice.

This article was originally posted by Dark Reading. Read the full article here.

Ransomware attack forces college to tell students to stay at home

A UK college says it has closed its campus buildings for one week, and advised students that all lessons and lectures will be taking place online, following a ransomware attack.

South & City College in Birmingham, which has over 20,000 students aged 14 and over, says that it suffered a "major ransomware attack" that has disabled many of its core IT systems.

As a result, yesterday the college informed students it was shutting its eight sites, and reverting to online teaching while IT specialists attempt to recover systems.

The news will cause further upheaval to college students, who only returned to face-to-face tuition last week, following an extended lockdown in the UK caused by the Coronavirus pandemic.

South & City College says it became aware of the attack on Saturday 13 March, and asked students to study from home:

"Our campus buildings will therefore be CLOSED TO STUDENTS for a week from Monday 15 March to allow our IT specialists to fix the issue.

"On Monday, March 15 we will revert to online teaching for the rest of the week for all areas. We are therefore asking you to access your online lessons from Monday, as you did during lockdown.

"There may be some disruption during this time and we ask that you please bear with us and contact your tutor you have any problems.

"Thank you for your cooperation and patience during this time. Keep an eye on our social channels for any updates."

Details of precisely which strain of ransomware has infected the college have not been made public.

The college says it has reported the incident to the Joint Information Systems Committee (JISC) Security Response Team, Action Fraud, Information Commissioners Office (ICO), the National Crime Agency (NCA) and the National Cyber Security Centre (NCSC).

Last September, the NCSC, in co-ordination with JISC, issued an alert and guidance for colleges and universities following a series of ransomware attacks.

Clearly that advice wasn't good enough to prevent South & City College Birmingham from falling foul of ransomware.

Ransomware victims in the UK education sector have included Dundee and Angus College, Newcastle University, Northumbria University, and colleges in Leeds, amongst others.

For more details, read the full article here.

Twitter Now Supports Multiple 2FA Security Keys on Mobile and Web

Twitter has added support for multiple security keys to accounts with two-factor authentication (2FA) enabled for logging into the social network's web interface and mobile apps.

"Secure your account (and that alt) with multiple security keys," Twitter said. "Now you can enroll and log in with more than one physical key on both mobile and web."

The company also announced a future option for 2FA-enabled accounts to use security keys as the primary authentication method while having all other login methods disabled.

"And coming soon: the option to add and use security keys as your only authentication method, without any other methods turned on," Twitter added.

Twitter has added support for using security keys when logging into mobile apps (Android and iOS) for 2FA-enabled accounts in December 2020.

2FA is an additional security layer for Twitter accounts that requires users to use a security key or enter a code on top of only entering a password to authenticate successfully.

This makes sure that only the owner can log in and block malicious attempts to take over the account by guessing or resetting the password.

While some high-profile Twitter accounts were hijacked last year even though they had 2FA

enabled after attackers could gain access to internal admin systems, users should still toggle 2FA to be better protected against less-sophisticated hacking attempts.

To turn on 2FA on your Twitter account, you will have to go to your profile menu into *Settings and Privacy*, then to *Security and account access* (desktop) or *Account* > *Security* (iOS) and toggle on *Two-factor authentication*.

This article was originally posted on Bleeping Computer. Read the full article here.

Product Updates

We have exciting new updates to share! Click below to learn more about what Inspired eLearning is doing to better our product experience for our customers.

LEARN MORE

Connect with us:

info@inspiredelearning.com I 800.631.2078
4630 N Loop 1604 W, Suite 401
San Antonio, TX 78249 USA
Privacy Notice