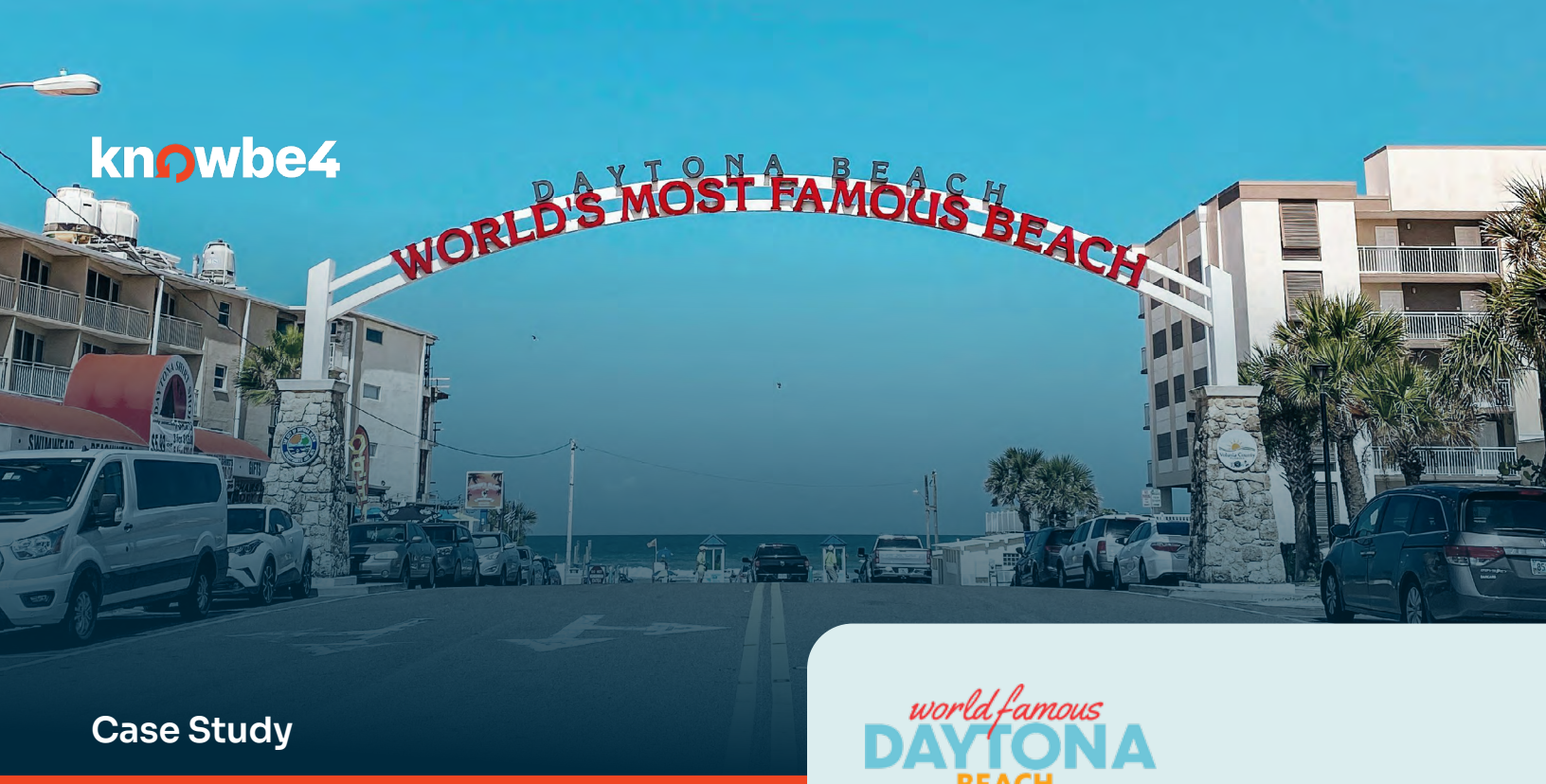


knowbe4

Case Study

world famous DAYTONA BEACH

Industry

Government

Location

Daytona Beach, Florida, USA

Challenge

Improving security awareness among city staff while keeping ahead of emerging threats

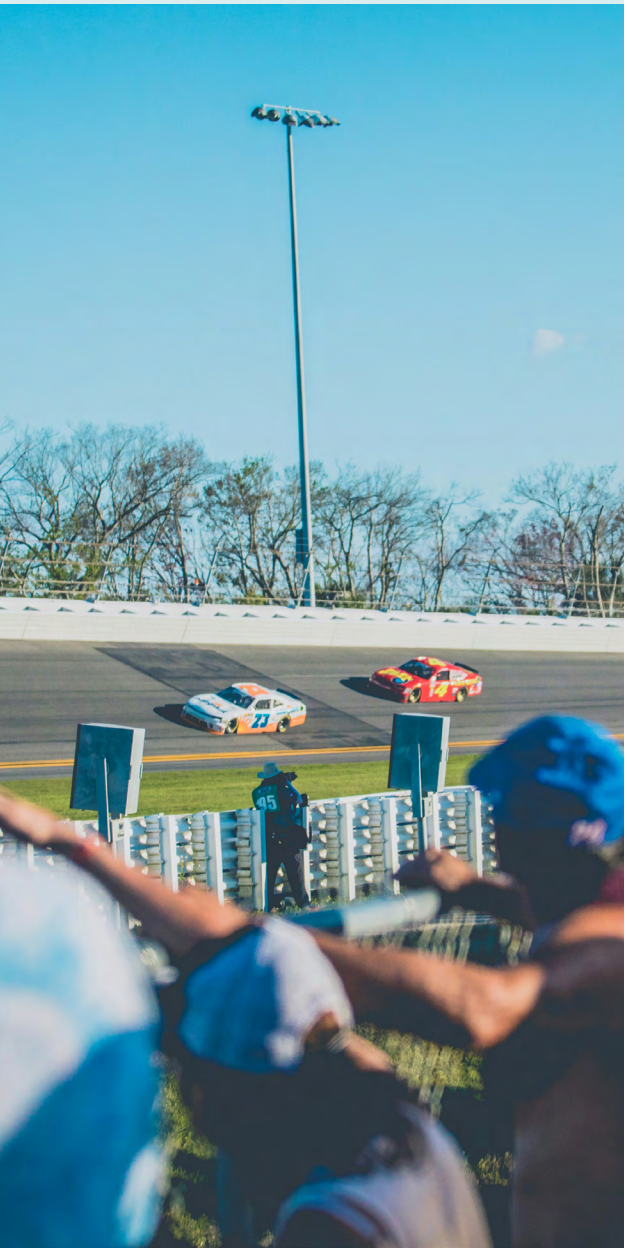
The City of Daytona Beach Transforms Its Security Culture With KnowBe4

As the home of NASCAR and the principal city of Florida's Fun Coast, Daytona Beach is always a hot spot. Its business and 85,000 residents rely on their local government for everything from planning permits and licensing to utilities and emergency management, and the City of Daytona Beach delivers these services to city dwellers as well as the 10 million visitors it welcomes each year.

With so much depending on it, the City of Daytona Beach can't afford to be the victim of cybercrime. Chief Information Officer Hossam Reziqa leads the team that manages and secures the city's servers and systems. As he describes it, his job is to ensure "our technology is working for us, not against us."

At a Glance

- **100%** security policy acceptance
- **2%** Phish-prone™ Percentage (and improving), down from **12%**
- **90%** faster emails recalls using KnowBe4's PhishER Plus



Moving Beyond Spam Filters

Reziqa recognizes that technology can be daunting for City of Daytona Beach staff worried about doing something wrong. Aside from using the right technology, his IT team must ensure staff are well trained so they can confidently get the most out of every tool and maintain a high security standard.

"Any fault in our technology or error from our staff could impact thousands of city residents," Reziqa says. "It is imperative that we are aware of what we have so we can secure our systems."

The City of Daytona Beach uses technology to their advantage, but they are fighting against a legion of cybercriminals who target a common vulnerability: the email inbox. Reziqa marvels at how quickly threats evolve and how difficult it is for a CIO to keep up.

"The trend of threats coming through email is very difficult to combat. You can't just depend on spam filters to identify those emails," Reziqa says.

That means they depend on its staff to make the right call about which emails to open and which links to click. It's a big responsibility, and the city didn't have an effective way to train users to identify phishing red flags.

When someone clicked a suspicious link, the IT team would have to engage in extensive one-on-one conversations reinforcing the city's security policy while manually working through the many steps to remedy the situation. All actions were reactive, taking place after the user had already been compromised.

It also took a lot of time — time the team couldn't spend fortifying the city's defenses.

Getting Proactive to Reduce Human Risk

Reziqa knew exactly how to address their email security issues. He'd had prior success implementing KnowBe4, and when he arrived at the City of Daytona Beach, it was an easy decision to onboard the platform.

"I have been a customer of KnowBe4 for at least 12 years," Reziqa says. "KnowBe4 is, hands down, one of the best platforms to train users on emerging threats."

He lists several KnowBe4 advantages that contributed to his past success, including:

- Simple implementation
- Well-structured content
- Ability to simulate realistic phishing attacks
- Automated, up-to-date training

KnowBe4's Security Awareness Training incorporates threats other customers have encountered and reported. It also boasts the world's largest library of new-school security awareness training content.

"A key benefit of KnowBe4 is the quality of the content, whether it is gamification, video, or the questions asked," Reziqa says, adding that he even finds some of the questions challenging.

The platform provides enough flexibility to customize and upload content to suit any organization's circumstances. Previously, Reziqa's team had difficulty knowing if all staff understood the city's security policy. By incorporating the policy at the start of staff training, the team increased confidence that staff read it because they had a log of who accepted the policy and when.

As an extra layer of protection, the City of Daytona Beach also implemented PhishER Plus, KnowBe4's incident response product, to automate threat detection and streamline incident response. The simplicity of PhishER's dashboards means the team can quickly get a comprehensive view of the security landscape.

"It's straightforward. All the information we need is available for us to make a decision and take action," Reziqa says.

They have come to rely on the Phish Alert Button (PAB) to report emails and PhishRIP to retract them. For Reziqa, who has had to recall emails in prior roles, PhishRIP is especially valuable. Recalling emails natively in Microsoft took over half an hour, but with PhishRIP, it's done within minutes.

"PhishRIP is so much easier. With a few clicks, you can pull that email back," Reziqa says, adding that the time saved by this feature alone is "extremely high."

PhishER Plus has helped the IT team increase their awareness and given them more tools to respond to attacks.

"We can see where the threat's coming from. We can see who's opened the email and reach out to them. This would not be possible without PhishER Plus."

> *"We can see where the threat's coming from. We can see who's opened the email and reach out to them. This would not be possible without PhishER Plus."*
>
> Hossam Reziqa, Chief Information Officer, City of Daytona Beach

Lowering the Phish-prone™ Percentage to 2%

Since implementing KnowBe4, the city's training completion rate has grown significantly. Department heads have bought into the program and lead by example, sharing when they've completed the training. Staff follow suit, and it's making a noticeable difference.

The city's initial phishing simulation revealed a Phish-prone™ Percentage of more than 12%. Today, that metric is down to 2% and continues to improve.

"Our users are learning to identify red flags in emails and we're seeing our scores improve, which is real data we can share with our leadership," Reziqa says.

From a broader perspective, giving staff the tools they need to identify malicious emails has fostered a proactive security stance at the City of Daytona Beach.

"KnowBe4 became not only a training platform, but also a tool for us to retract emails, identify risks, and examine details," Reziqa says. "It's an integral toolkit for our team to fight cybercrime."

> *"KnowBe4 became not only a training platform, but also a tool for us to retract emails, identify risks, and examine details. It's an integral toolkit for our team to fight cybercrime."*
>
> Hossam Reziqa, Chief Information Officer, City of Daytona Beach

Throughout Reziqa's 12-plus years using the platform, the KnowBe4 team has been by his side at every step and are responsive to his suggestions. "The customer support from KnowBe4 is second to none," Reziqa says. "We've never had a situation where we couldn't get an answer immediately."

Regardless of Reziqa's role, that partnership with KnowBe4 has enabled him to strengthen defenses in any environment.

Transforming the Security Culture

KnowBe4's ultimate impact is how it has transformed the security culture at the City of Daytona Beach. By using KnowBe4, the City of Daytona Beach has boosted security awareness and empowered Reziqa's team to become more proactive.

"Our users now pride themselves on the security certificates they get," Reziqa says. "Their peers are calling them out and recognizing them for emails they caught."

In his time using KnowBe4, Reziqa has witnessed the platform's capabilities continually grow. And having seen what's to come, he can't wait to start implementing the new features.

"I recommend KnowBe4 to any organization that uses email," Reziqa says. "And today, it's difficult to find an organization that doesn't."

0625-US

knowbe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com