ENGAGING THE AUDIENCE

Leveraging gaming as an engagement channel

H2 ACT PLAN TRACK PARK OPP THR NEU

Research on the world of gaming indicates that 81% of internet users game on at least one device each month. Amongst 16-24 year olds, the number rises to 91%. The increase in online multiplayer games that put the gamer at the heart of the experience (like Overwatch and Fortnite) has accelerated interest.

4 in 10 gamers actively follow esports, watching both live streams and tournaments and broadcasting their own gameplay. The individuals at the forefront of esports, dubbed "E-Athletes", are influential celebrities in their own right. Tyler Blevins, a leading E-athlete, accumulated 22 million subscribers on his YouTube channel in 2019, and signed with Adidas as a brand ambassador in 2020.

No wonder then that brands like Amazon, Google, Facebook and Apple are making big bets on gaming as an engagement channel for delivering live streaming, sponsorships and product placements.

In January 2021, the United Nations Development Group (UNDP) and University of Oxford published the the results of the Peoples' Climate Vote, a survey of public opinion on climate change. Poll questions were distributed through advertisements in mobile game apps in 17 languages, which resulted in a huge, unique, and random sample of people of all genders, ages, and educational backgrounds. 1.2 million people from 50 countries responded, making it the largest survey on opinion on climate change ever conducted.

CYBER RISKS

Cyber security training is essential

H1 ACT PLAN TRACK PARK OPP THR NEU

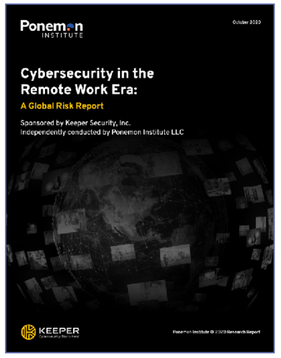
One in three UK workers are currently based exclusively at home. It's the same in the US and it's creating a major headache for IT security teams. One in five UK home workers has received no training on cyber-security, according to a November 2020 survey. The survey also found that two out of three employees who printed potentially sensitive work documents at home admitted to putting the papers in their bins without shredding them first. A separate UK study from April 2020 found that 57% of IT decision makers believe that remote workers will expose their firm to the risk of a data breach.

Companies need to ensure that

- All staff are using a dedicated and correctly configured work laptop. Personal laptops - particularly those shared by other family members who may be gaming or downloading from file sharing websites - must be regarded as insecure
- Remote computers have secure and encrypted connections through a VPN or virtual private network, not a personal one that may be infected with malware
- Staff are fully aware of - and do not act on - "phishing" emails designed to trick someone into handing over sensitive data or downloading malware
- All staff receive proper cyber-security training
- Firms have policies in place so that staff know who to immediately report a threat to and that they are not afraid of repercussions - which might lead them to cover up mistakes

Cyber security expert Tim Sadler, CEO, Tessian, notes: "Time and time again we see how simple incidents of human error can compromise data security and damage reputation. The thing is that mistakes are always going to happen. So, as organisations give their staff more data to handle and make employees responsible for the safety of more sensitive information, they must find ways to better secure their people. Education on safe data practices is a good first step, but business leaders should consider how technology can provide another layer of protection and help people to make smarter security decisions, in order to stop mistakes turning into breaches."

FURTHER READING



TECHNOLOGY HOME PAGE