Article

Oct 2022

Sport and cyber security

How can these things possibly be linked? A Sunday league kickabout, summer cricket tournaments and community netball matches aren't strong candidates for a cyber threat, right? Wrong.

Scott McNab
Information Security Consultant

Email scott.mcnab@waterstons.com

According to a 2020 survey by the National Cyber Security Centre (NCSC), 70% of sports organisations have experienced some form of cyber breach or incident.

Within these:

- 30% resulted in direct financial damage – averaging over £10,000 per incident (with the largest £4million)
- 37% directly experienced data loss
- 75% were victims of phishing through fraudulent emails, texts or phone calls

As sport, technology and the way we communicate become more sophisticated and technological, cyberattacks will only continue to increase, with hackers focusing on what they stand to gain regardless of club, sport, or size.

How have sports clubs been hacked?

Football, understandably, is a popular target with none other than Manchester United being disrupted for several days (and likely suffering financial loss although this has not been reported) due to a suspected ransomware attack.

Another English Football League club suffered a severe breach to their internal IT systems via a phishing email, or using remote access through the club's CCTV, meaning their turnstile system was locked out by a hacker. With no supporters able to enter the ground a scheduled fixture was nearly cancelled, which could have resulted in fines of hundreds of thousands of pounds from the English Football Association. It has been understood that the hackers demanded a ransom of 400 bitcoin (over £300,000).

Could this be avoided?

Both of the cases above – and many more – could be avoided by appropriately training relevant people in what to look out for a cyberattack, and how to deal with it.

But it's not all about staff training as even the most fastidious can make mistakes, so we've put together…

Waterstons top tips

1. Be strong

Ditch the conventional methods of creating passwords and use 'passphrases' which consist of 3 or more random words that cannot easily be guessed. For example, BallPosterSquirrel.

2. Be phishing aware

Always think before you click. Hackers play on the emotions of their victims so anything requiring urgency, greed or guilt should ring alarm bells. Supplying personal information, bad spelling and grammar and unusual email addresses are also red flags.

3. Be up to date

Make sure your operating systems and software have the latest updates and patch versions installed as older versions can become entry points for hackers.

4. Be in the frame

Following the latest guidance and/or frameworks from reliable sources can make sure you're aware of the latest incidents and advice. Make sure you regularly check out the National Cyber Security Centre website, or even consider adopting a framework like Cyber Essentials to ensure your club is aligned with best practices.

Sport brings together people from all walks of life with one common interest to create unforgettable moments. Hackers know how to use that to their advantage – it's up to us to make sure those unforgettable moments remain in the game, not in cyber incidents.

To find out more about cyber security options for your club, how our team of experts can help to make sure you're onto a winner through training (like we did for Morton in the Community), frameworks or an audit get in touch by emailing scott.mcnab@waterstons.com or calling 0345 094 0945