

'We think like the bad guys to stop cyber crime'

BT's deputy cybersecurity officer, Steve Benton, tells Emma Deighan about fighting digital crime

STEVE Benton, deputy cybersecurity officer at BT, says he is always in the mindset of a cyber criminal.

His job is to "detect, protect and recover from cyber and physical situations here and across the world" for the telecoms giant.

The role is about "looking after our people, our assets, our exchanges, engineers out on the road and our retail shops in the real and virtual world".

"We're always kept on our toes," says the Bangor man.

"Many years ago, you had to worry about hacktivists disrupting services but that has grown markedly. Criminals have now realised there are identities online and there is a lot of money to be made at relatively low risk. It's become a seriously big business and globally it's worth £4trn," he says.

The sophistication of cyber-crime gangs increases at the same pace as technology. "They operate like a business model so I have to put myself in their shoes," says Steve.

At BT in Northern Ireland, around 300 people work on combating cyber crime. That number grows to 3,000 internationally in the 170 countries where BT has a presence.

"We see fraud or scams aimed at an organisation and the criminals will have done the research to identify things like employees who work together closely and pose as close colleagues and try to persuade in what we call whaling or spear fishing.

"They are getting smarter because of the money that they're making and then they have that money to invest and plough back into cyber crime," Steve explains.

BT's cyber crime team is made up of two divisions; the red and blue teams. Reds pose as attackers and blue are the defenders.

"When we come together, we

make purple and that's a victory for all of us," says Steve.

"The red team are very highly trained hackers. They do cyber hacking and human targeting and their job is to stress test potential weaknesses."

As the Covid-19 pandemic forced many businesses adopt remote working for employees, having reliable cyber security measures in place is more important than ever.

"The one thing that organisations need to recognise is that there is never 100% security and there never will be and we have criminals innovating all the time, constantly in a race so we have those multiple layers of protection to stop an attacker at some point in their attack," says Steve.

"I think today the need for good security has been accelerated by the move to working from home. For most organisations there has been a digital transformation so businesses need to reassess what their security posture is now.

"They have changed what their organisation looks like and how it works now and security is an issue that needs addressed because there wasn't the time to fully think through those changes at the beginning of lockdown."

Steve talks passionately about the cyber security sector. It reflects his passion for the whole IT world, a passion which goes right back to his childhood.

He has two daughters. Sophie, an undergraduate at Queen's University, Belfast and Charlotte, a pharmacist.

Steve was first introduced to technology by his brother's friend when he was a child.

He grew up in Ballyholme, and recalls his first computer, a Sinclair ZX81 with 1KB of memory.

"My brother's friend brought it round and showed me what it could do and I thought it was really interesting so I joined a computer club at Bangor Gram-



mar school and my dad saw that interest and really supported me and bought my first computer in 1983."

A bit of self-teaching in learning the basics as well as an O-level in computer science followed, pushing Steve's fascination with all things techy further.

"I then went on to do a degree in computer science and electronics at Queen's University. That was all about how the chips inside computers work and how they communicate. It was a very innovative degree taught across two faculties," he adds.

He came out with a first in the degree but it was his sandwich year at a new BT centre here that saw him go on to spend much of his career with the telecoms giant.

"That was a new software centre that opened with support from Invest NI. I did a year out there and they treated us well. I did decent work and that fired me up and I thought this is what I want to do so I came out with a first and was writing software for a few years of my life."

Automated banking followed, as well as some high pressured work on the trading systems in the stock exchange.

Steve would go on to work in various roles at BT as well as

Cyber chief:
Steve Benton works for BT

with some of its venture organisations and five years ago he was brought in when BT invested in its security response.

He worked with a colleague to create an 'annual security programme' which he says: "takes the approach to thinking like the bad guys".

"We look at those multiple layers and how to get on the front foot to understand a threat," he says.

When explaining the sophisticated setup in place at BT to protect its data and identities, Steve breaks the process down into three parts.

"What they want to do is monetise what they have achieved from you," he says of the hackers. "So when I'm looking to defend against that we look at expensive, dangerous and worthless.

"Expensive is the amount of investment an attacker will make and I want to make it as difficult as possible for them. We do that by getting the basics right and the hygiene around our security. We have different layers of defence too so an attacker needs to get multiple things right all of the time and if when they fail my team will be on top of it.

"Then we have dangerous, which is using everything we can to understand who that

attacker is, where they have come from and do they look like someone we've seen before. We'll gather that evidence and pass it across to other agencies to make the lives of those criminals much more challenging like restricting their abilities to travel. We can add to the pool of information the police has, and internationally what bodies like the FBI have."

Steven finishes off with the 'worthless' element of the process, adding: "That's a payout piece. They don't get away with what their objective was and they don't get to trade information they get from my company. Your information is not going to get compromised through organisations like ourselves but if your information is stolen elsewhere those credentials could end up on the dark web."

Today, Steve's environment may have changed as he swaps the BT HQ for his home in the Ards Peninsula, but the work has certainly not and if anything, it has ramped up as the whole of society gets to grips with a more digitally reliant world.

He adds: "As a team we have worked hard over lockdown to make sure our broadband is strong at a time when communication technology is more important than ever."

The need for good security is more important than ever