# Cybersecurity for Charities: Is Your Non-Profit At Risk?

**Despite all the good they do, the non-profit sector is a prime target for cybercriminals, which is why cybersecurity for charities is so important. With an annual income of over £69 billion in 2019, attacking charities has proven to be a lucrative endeavour for cyber-criminals, and they're not slowing down any time soon.**

Over a quarter of charities in the UK said that they'd experienced some kind of cyber breach this year, according to the Government's Cyber Security Breaches Survey 2021. Among those who did, 18% lost money or data because of the attack. In recent years, there has been a number of high-profile cyberattacks on charities, including an attack on Blackbaud software used by many non-profits in 2020, and a ransomware attack on the Salvation Army in 2021.

One of the most notable breaches was the notorious "WannaCry" ransomware attack on the NHS in 2017. Countless organisations were affected, with global costs of up to £6 billion, however, the NHS suffered one of the largest impacts, being brought to a standstill for several days. The exact cost of the attack is unknown, but it's believed to be around £92 million. Most importantly though, invaluable NHS services were restricted, and no doubt the real cost of the attack included patients' quality of life.

You might think that charities would be off-limits to hackers, but unfortunately, threat actors don't care who they hurt. In this blog, we'll explore several security vulnerabilities that tend to be common in this sector and give some helpful tips to help charities protect themselves from cyber-attacks.

## Is Your Organisation Vulnerable?

One of the main reasons why non-profit organisations often fall victim to cyber-criminals is because of a lack of resources. When your aim is to support vulnerable people, or provide a necessary service, it's unlikely that you'd want to allocate funds for processes that aren't directly advancing that aim. However, when your cybersecurity budget is low and security practices are neglected, one immoral threat actor can bring the entire organisation down.

As charities often employ volunteers and people on temporary contracts, onboarding can be another issue. People coming and going or working on an ad-hoc basis often results in it being much more difficult to keep track of staff activity, manage logins and access, or deliver effective security training to everyone in the team.

Unsecured BYOD also poses a huge potential threat to charities. If your non-profit organisation lacks the large tech budget to provide staff with secure company-owned devices, most team members will be using their own phones and laptops. The danger with this is that those devices could house easily exploitable apps that become a hacker's gateway into your organisation. Also, simply struggling to keep an account of devices and what protections they have (if any) is an additional risk.

While there are obvious differences, one thing about cybersecurity for charities that is very similar to the for-profit sector, is that most of the cyber-incidents reported happened as a result of a phishing attack. When working from home or on a volunteer contract – as is often the case with charities – team members tend to lower their guards and be a little more distracted, making them more likely to click a suspicious email link without thinking of the consequences.

## Why Hackers Target Charities

When it comes to cybersecurity for charities, the unfortunate truth of the matter is this: non-profit org are like sitting ducks to hackers, so why would they turn down such easy prey?

Cyber-criminals are ruthless and don't care who they harm. These threat actors have no moral compass, and this is evidenced with their previous attacks; targeting healthcare providers and targeted other essential services like schools and councils. It's safe to say they're not going to draw the line at charities.

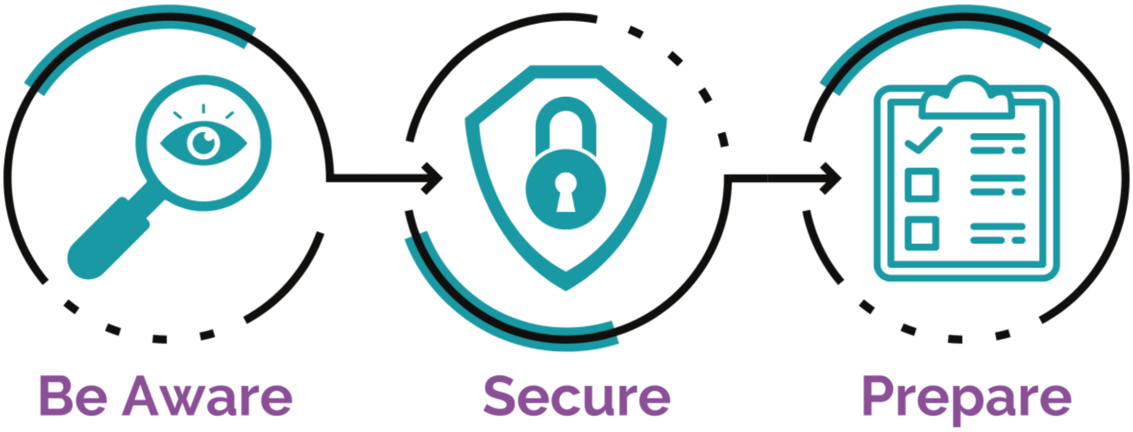
So, why would a criminal target a small charity as opposed to a large organisation? Simply because it's easier, often for the following reasons:

- Rather than hacking one big business, it's often more profitable for a hacker to attack a handful of charities in succession.
- Getting through the security defences of a large-scale company will usually require a lot of time. But in the case of non-profits with a small tech budget and minimal cybersecurity awareness, it's like shooting fish in a barrel.
- Hackers don't need to be an expert to crack basic passwords or send a half-decent phishing email, so there's way less technical knowledge required to hack into a small charity, which opens the floor to a larger group of less-skilled criminals to try their luck.

## Defend your Organisation

To continue providing vital services and support to vulnerable people and boosting awareness for important causes, charities must protect their systems. Cybersecurity for charities can sometimes be daunting, but staying safe doesn't need to be convoluted or confusing.

**We've broken down the route to strengthening your systems into 3 easy steps:**



**Be Aware:** Learn of the risks and how to spot them. Educate your team on what motivates threat actors, the organisations that they've targeted, and how they could take advantage of security vulnerabilities within your systems. Developing an awareness of any potential security threat within your current environment will take you one step closer to closing those gaps and fortifying your organisation overall.

**Secure:** Once you know what the risks are, mitigate them via robust security solutions and services. Strengthen your systems using anti-virus technology, strong firewalls, and VPNs. Implement a secure password policy, improve your onboarding strategies, and make sure that all members of staff and volunteers have a responsibility to uphold the security of your organisation. In other words, put up the best defences you can with the budget you have.

**Prepare:** This may sound counter-intuitive at first, but assume that the previous two steps are going to fail, and act as though you've already been breached. This means updating your incident response plan, limit user access to only what team-members need to do their job (because the less admin-level users with access to your entire system, the better), and invest in penetration testing that can give your organisation an idea of whether or not a hacker can infiltrate your defences, and what they could do to your system once they're inside.

For more information about **Be Aware/Secure/Prepare** stay tuned for our next blog post, where we'll go into more detail about the steps charities can take to protect themselves from threat actors. In the meantime, if you're a charity that requires more hands-on help, take a look at our Charity Support Fund which enables charities to strengthen their security via pro-bono testing and training.

**If you represent a charity that requires some extra security assurance, please contact us today and enquire about our pro-bono work. Alternatively, if there's a cause that's close to your heart that could benefit from our services, enquire here to let us know about your chosen charity, and we'll see what we can do.**

**Want more info on cybersecurity for charities? Read our Case Study about a pro-bono penetration test we did for a good cause here.**