BIZCOMMUNITY

5 things small business owners can do to avoid cybercrime

By Quentyn Taylor

23 Nov 2020

Cybercrime has advanced to a stage where hearing about large corporations experiencing cyber attacks is no surprise. It could be very easy as a small business to have sympathy for those corporate firms, but ultimately feel thankful that your organisation is small enough not to warrant you being a target for this kind of activity. This sort of thinking, however, is a costly mistake.

Quentyn Taylor, director of information security at Canon | image supplied

Yes, for those cybercriminals who are focused on the high-risk equals high reward dynamic of targeting high scale corporates, you may not be of interest. But this is not the only type of assault a business could face.

We're seeing an increasing number of large-scale, low-risk operations, where the individual 'rewards' for the attacker may be fairly small, but when this is spread across a wide net of businesses, the payoff begins to mount up. And this makes it a very easy win for these attackers, but a nightmare for small businesses. We all think it won't happen to us until it actually does.

Although there are new scams being invented every day, there are currently two main types of approach in this situation, so it's worth taking note.

The first involves businesses being sent an email or a physical letter from a supplier claiming that they have new bank account details and requesting that the business updates their systems accordingly.

The result is that a small organisation follows what it believes to be genuine instructions and ends up paying an attacker any funds due to that supplier. And even worse, the business still remains liable for paying the genuine supplier once it is discovered that the money has gone elsewhere.

6 ways to safeguard yourself this Black Friday, Cyber Monday

Nithen Naidoo 17 Nov 2020

The second involves an attacker gaining access to a small firm's systems and changing their invoicing account details to the attacker's own account details. That means that any customers receiving and then paying those invoices are giving money straight to the cybercriminal, leaving both customer and business out of pocket, and the business liable for the customer's funds going elsewhere.

These types of attack are so easy to carry out and hard to trace, but that doesn't mean there's nothing you can do to protect yourself. In fact, there's plenty you can do. The key is not to get complacent and ensure you have robust security protocols in place to protect your data.

Here are five things small business owners can do:

1. Remember that any device connected to the internet poses a potential risk. Ensure you have multi-factor authentication in place for any part of your business that is connected to data and exchange of information.
2. Make sure you clearly understand your business processes, such as how you're invoicing, so you can be more aware of where an attack might come from. Also be aware that the more informal your invoicing system is, the easier it is for a cybercriminal to access and start changing details.
3. Don't be afraid to ask thorough questions of anyone requesting you share information with them. Like someone claiming to be from your bank's fraud department, for example. Double-check account details. Call suppliers and customers back using a phone number you know is genuine to check incoming .requests.
4. Don't think it won't happen to you. Stay vigilant and train your team on the risks.
5. Plan for the worst-case scenario so you know what steps to take if you do suffer a breach.

ABOUT THE AUTHOR

Quentyn Taylor is director of information security at Canon.