Like every other company in the world, cyber criminals also take their work as a business and look for ways to boost their sales. Ransomware is a profitable way for them to earn through cyber crimes, which forces their victims to pay a certain amount of money. To increase their earning, cybercriminals are learning sales tactics used by legitimate corporations. Unskilled cyber criminals are outsourcing phishing, botnets, and ransomware attacks to skilled hackers. With help desks, money-back guarantees, and multiple payment options, and latest [technology](http://www.cardzgroup.com/ContactSmartCard.html), ransomware has now become a full-scale business in the world of cyber criminals.

The following are some of the ways cybercriminals use sales best practices to carry out ransomware attacks:

1. **Defining the Target Audience**

Just like any other sales campaign, cybercriminals also start by defining their target audience. The target audience in this context means victims who can be potentially forced into paying the ransom. Cybercriminals conduct research and look for organizations in different sectors that are most likely to pay a ransom amount in return of getting their services and data back. For this, they use social websites such as Twitter and LinkedIn to find vulnerable employees that can be targeted easily.

1. **Launching the Campaign**

For a cyber attack to be successful, hackers need clear insight into the targeted organization. They look for exploitable vulnerabilities and locate critical infrastructure and assets. Just like any other sales and product marketing email, they will carefully craft a phishing email with a message that is attractive enough to entice a user into acting upon it. Regular email marketing campaigns [average opening rate](https://www.campaignmonitor.com/resources/knowledge-base/what-are-the-average-click-and-read-rates-for-email-campaigns/) is about 15 to 25 percent, whereas the average rate of opening phishing emails is [30 percent](https://www.phishingbox.com/news/phishing-news/verizon-data-breach-investigations-report-summary-2016).

1. **Providing a Free Sample**

Sales teams usually provide free trials or samples to interested customers to turn them into actual customers. In a ransomware attack, cyber criminals use similar strategy and prove to the victim that they can recover their compromised network by providing them a sample of their stolen data. The victim agrees to pay higher ransom to recover full data, where [1 percent](https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf) of criminals don’t decrypt the data even after receiving full amount of ransom.

1. **Using Peer Pressure and Social Engineering Techniques**

Sales tactics such as one-time only sales, limited edition, or exclusive product and coupon releases have been very effective in making the recipient act on emotion before thinking logically and making more informed decisions.

Cyber criminals use the same peer pressure techniques that make the victims overlook otherwise obvious defects in their messages, such as using fear of blackmailing or embedding malicious links in fake termination emails.

1. **Providing Services at Professional Level**

Lastly, cybercriminals with skills and experience have been selling services to others that are looking to threaten a third-party. Moreover, they even provide customer services support and are also open to ransom negotiation in certain instances.

**How to Fight Back at Corporate Level**

With more sophisticated tactics, professionalism, and increasing incentives for cybercriminals to carry out ransomware attacks, what measures can your organization take? The following are some recommendations that can help decrease the impact and risk of a ransomware attack.

1. **Keep Your Security Tools Upgraded**

Apart from setting up anti-malware and patch management programs, you need to take your security to the next level with additional tools such as:

* Phishing simulation campaigns to test your employee’s susceptibility to phishing emails.
* Data loss preventions tools to detect emails with potential red flags.
* Enhanced email applications and firewalls to carry out deep inspection of email and web traffic for unusual malicious behavior.
* Server and end-point heuristics to identify unfamiliar processing demands or API calls.

1. **Conduct Regular Security Trainings**

Majority of successful attacks are a result of human error. It is important to regularly train employees on techniques used by cyber criminals to attack and exploit vulnerabilities. Educate the staff on different types of attacks, the methods used to gain attention and how they need to respond to unusual phone calls, text messages or emails. Share examples of past attacks and phishing emails.

1. **Keep your Incident Response Plan Updated**

Even with all the security measures in place, a ransomware attack can still happen. Hence, it is important to ensure that you have an incident response plan to help you quickly respond to a ransomware attack. It should be regularly updated so your staff is aware of the action plan when required.

**Conclusion**

Ransomware attacks are very likely to stay for now, considering the fact that they are becoming profitable businesses for cyber criminals. However, by understanding the tactics used, we can prepare our organization proactively to minimize the associated risks.