

Cybersecurity Investigator 1

Ransom Cards

<p><i>Ransom Card</i></p> <p>If we pay the hackers what they ask for, we will only give them more resources to carry out more crimes in the future. Giving them money will convince them that their plan works, and it might even help them create stronger ransomware programs.</p>	<p><i>Ransom Card</i></p> <p>The encrypted data is extremely valuable! Comparatively, the ransom amount is likely far less than what it would cost to recover this data and redesign the databases and websites.</p>
<p><i>Ransom Card</i></p> <p>Some strains of ransomware have coding and encryption errors. If this has happened in our case, then even paying the ransom won't decrypt our data, and we will be unable to access it indefinitely!</p>	<p><i>Ransom Card</i></p> <p>Often the malware creator's only real goal is to scare people into paying. The criminal never intends to let his or her victims decrypt any of the encrypted data. A recent report claimed that only 19% of ransomware victims who pay the money actually get their files back.</p>
<p><i>Ransom Card</i></p> <p>Much of our city's data is highly confidential. We don't want someone else to be in charge of our data. The only way to gain control back might be to pay the ransom.</p>	<p><i>Ransom Card</i></p> <p>If it comes out that our data has been hacked, we might be sued or have to pay additional fines. If we decide to pay the ransom, we may be able to keep news of the breach private!</p>
<p><i>Ransom Card</i></p> <p>Criminals use bitcoin for money transfers because it is harder to track than conventional payments. It is also easily transferable between countries because it bypasses banking systems. If we pay the ransom, we will not be able to track where it goes and therefore will not be able to get it back.</p>	<p><i>Ransom Card</i></p> <p>If we do not have back-ups of our data readily available, then we do not know whether we can ever get the data back without paying the ransom.</p>