Ryan are mildly educated about cyberspace tend to

Economics, Trade

Ryan MatheuP. I. D. #: 3611448Finding Fresh IdeasValuing InformationSecurity from a Phishing Attack In the world of cybersecurity there willalways be people who threaten your privacy and will try to steal sensitiveinformation from you, in order to either sell it or use it with malice. Thebiggest problems with user's and how they protect themselves in cyberspace, isthat they either believe they aren't at risk or use the tools incorrectly, leaving them vulnerable. As has happened to me, many users often times decideto bypass certain security measures put in place by either the OperatingSystem, System Manufacturer, or installed by them, in order to access certainwebsites or games online. The problem here is that many user's make trade-offsin certain situations; such applies when choosing certain security software.

In many cases, according to the article theamount of security people are willing to invest in directly correlates with theamount of knowledge they have about cyberspace. People who are less informedtend to either not take any security measures, or feel they aren't vulnerable. People who are mildly educated about cyberspace tend to take the middle groundand implement firewalls, at the very least. Where people who are more aware ofcyberspace and tend to value their privacy and security, will often makesacrifices in terms of money, latency and productivity in order to ensure theirsecurity online. A common mistake made by user's aswell is that if certain programs or web applications don't work due to afirewall/antivirus/anti-fishing software being in place is that they mayall-together disable it in order to gain access.

What they don’t realize, oroften times brush off, is that by disabling these security measures, even foronly a few minutes makes all of their information vulnerable. Often times, games use certain ports, and people may even open certain ports in order toallow the game to function properly. This is a problem because a port left opencan easily be used in order to penetrate the system. This article mainly covers thesacrifices that must be made by a user to ensure they system is as secure aspossible.

These trade-offs, as listed above, include cost, latency, efficiency, and productivity. The average computer user is not willing to pay a highpremium for higher latency, even if it means a more secure system. On thecontrary, those who are willing to pay high premiums, are willing to havehigher latency times, or wait times, and slightly lower productivity, butknowing their systems are secure gives them peace of mind.

The study found thatmost people fall under Pragmatists, between 59% – 73. 2%, as people who do infact want better cyber security but are not willing to sacrifice efficiency andlonger wait times, or latency, to get it. Online between 19. 1% and 26.

8% ofuser are willing to have higher latency and less productivity in order toensure their systems remain secure. Lastly, are the minority of people, whichare those that are unconcerned of their systems integrity in cyberspace, whichare labeled the Unconcerned in the article. These are people that essentiallyaren’t willing to make any sacrifices to productivity or latency, for anyamount of money, as they see security measures as

obstacles to using acomputer, and just something which will “ slow it down”. Based on this article I would saythe most important thing is to ensure that the security measures you use onyour personal or work machines are able to provide you with sufficient productivityand low enough latency where you can get work done, but enough security toensure you’re safe. It seems to me that many people may tend to not think longterm, as they don’t see that slightly longer wait times now and slightly lessproductivity, means more security.

In the long term, they just about break evenin terms of efficiency; as if your system gets hacked, it will take aconsiderable amount of time in order to restore information, not to mention thehassle of changing information if it gets stolen. This is of course assumingyour information can be changed, example in point would be social security. Inconclusion I would advise users, whether it be for home or business use, tofind an adequate middle ground in terms of cost, efficiency, latency, and productivity, where you are still protected very well. A little extra time each day, toensure security, will pay itself off in the long term, to not have to deal withthe aftermath after being hacked. At the end of the day, people tend to go tocompanies they can trust, if you get hacked, chances are you will lose at leasta portion of your clients, which is very bad for current customers, and futurecustomers as well.

Link to Academic Article: https://academic. oup. com/cybersecurity/advance-article/doi/10. 1093/cybsec/tyx006/4055925