How to Protect Yourself Online

September 27, 2019

There has been no shortage of news about online privacy. Whether it is big tech gaining a bigger hold on our private lives or hackers stealing personal information both at the corporate and individual levels, data seems to be at risk with every click of the mouse.

The risks are growing at a faster clip as more and more processes become automated, providing multiple points of entry for hackers and other entities to compromise private data and perhaps, carry on undetected. More than half of small and mid-size businesses have been the target of some sort of cyber crime.

Ransomware attacks, in which users are blocked from accessing their data until paying a ransom, more than doubled in the first quarter of 2019, compared to 2018's first quarter — while the average ransom payment has also nearly doubled.

Individuals, businesses and municipalities have all been targeted by ransomware attacks. Arizona Beverages saw its sales halted for days due to an attack, while aluminum producer Norsk Hydro lost $52 million in an attack. And then there's the City of Baltimore, which estimates an $18 million loss from an attack that occurred in May.

The total damage of these attacks — some of which will garner more attention than others — is expected to top $11.5 billion this year.

With the widening scope of these attacks, it's not surprising that people and businesses may feel powerless to stop them. But that's not to say precautions can't be taken. For businesses, that means that data security can no longer be thought of purely as an IT function. Each department in the supply chain must take measures to ensure data safety and to quickly rectify any breaches.

For individuals living in a world of e-commerce, online banking, and social media, there are measures that can be taken to limit the potential for breaches and mitigate the scope of losses.

A few tips to protect personal information online:

1. Think twice before giving personal information to conduct business: If ordering items online, one will surely have to hand over payment and address info. But there are other times when companies may ask for information for their own marketing purposes, in which case, decline. The same can be said for answers for security questions. There rarely is a need to actually provide the mother's maiden name or home street for security, the key is to provide answers to help you access your data.
2. Be wary of free Wi-Fi: When traveling, free Wi-Fi can seem like a godsend, but it provides a portal for others to track internet usage. If it is crucial to use public Wi-Fi, limit online activity only to what is most essential — ideally not checking bank information, for example.

3. Don’t open suspicious emails or attachments: Hackers have gotten very good at sending real-seeming emails from business and personal accounts. Remember that most companies will not send out-of-the-blue requests for personal data. Also, be cautious opening emails from known contacts that seem to be a little off. For example, if a known contact sends a blank email with an attachment, it is better to call the person to confirm they sent it than to assume it is safe and get hit with a virus.
4. Lock your tech devices: A laptop or phone left unattended for just a few moments can be a treasure trove for data thieves if not protected adequately.

For more information and to discuss proactive steps that can be taken towards protecting important data online, contact your Anchin Relationship Partner or Russell Safirstein, Partner in Charge of Anchin Digital Risk Solutions at 212.840.3456 or info@anchin.com.