Family Office Insights

Practical Tips for Cybersecurity While Working From Home

In these unprecedented and uncertain times, with practically every state operating under a shelter-in-place or stay-at-home order, and entire segments of the workforce now working remotely, businesses – as well as family offices and their family members – have had to adapt to a new operational reality.

Not to be outdone, cybercriminals have also adapted to this new reality just as quickly, with new and inventive ways to attempt to exploit any weaknesses in your cybersecurity. Now that we have had a few weeks to begin to get acclimated to this new way of working, and since it appears that many of us may be working from home for the foreseeable future, we have assembled some of our top helpful and practical tips for maintaining the cybersecurity of your family office while you work from home.

We hope these tips will help you identify and minimize the risks of possible threats to your family and your family office. Some of these are precautions that will sound familiar from your workplace environment, but the rapid development of threats to your "new office" requires that you be even more vigilant. As the current state of play continues to evolve, we all have to take extra care when it comes to the technology we use and how we use it.

Phishing Threats

Phishing emails are nothing new, and are a familiar threat in the modern business environment. Nevertheless, with the coronavirus disease 2019 (COVID-19) pandemic at the forefront of everyone's mind right now, and the news cycle constantly pushing out updates on the latest developments, cyber attackers are looking to take advantage. Be watchful for potential phishing emails trying to convince you to submit credentials or download a file in order to gain access to the latest information on the virus or benefits under the CARES Act. You should also be wary of emails appearing to come from even the most authoritative sources on the virus, from trusted companies touting the latest updates on protocols or procedures, and even from your colleagues and contacts asking you to download an attachment and send it back to them under the guise of having trouble with remote access from their phones or other devices. Pay close attention to the actual email address of the sender – not just their name – check email headers and domains names, confirm whether the email is coming from a sender you know or contains information you solicited, and be on the lookout for anything that otherwise seems odd about the email (e.g., are they trying to get you to open an attachment, do they address you using uncharacteristic formality or informality, is email an unusual way for them communicate with you, etc.?).

Network Connections and Software Updates

Given that the level of IT infrastructure at your home is probably nowhere near as high as it likely would be in the office, work via a secure connection established by a virtual private network, or VPN, whenever possible. Since all of your devices (personal and business) will be using the same network and passing data through the same router, which are potential gateways for hackers, ensure that you keep the software on all of your devices up to date. Software providers regularly use updates to address security gaps, and enabling automatic updates where you can is always a good practice. In addition, you should turn on the encryption options on your router, which will scramble information sent over your network.

Keep Devices Separate

Although most of us have never had quite this much unavoidable overlap between our personal lives and our work lives, try to keep the lines from blurring between your business devices and your personal devices. This might be easier said than done, as all of your activities are now taking place in the same general vicinity, but by keeping things separate, you can avoid unintentionally transferring any work data to your personal devices, which are, in most cases, much less secure. This will also help protect your personal data if your work device is targeted and hacked, and vice versa. In addition, spam that uses data from your social media accounts and other personal web browsing allows hackers to target you more efficiently with emails that you are more likely to be enticed to click on from your work computer or that appear to be from colleagues, personal contacts or other trusted sources (e.g., your online bank, your credit card company, the online retailer where you just placed an order, etc.).

Virtual Meetings

With Zoom and similar platforms being all the rage, and millions of people now using video conferencing services, hackers, too, have found ways to use those platforms for their own benefit. It is important to verify all participants in teleconferences and video conferences to confirm that no unauthorized individuals are listening in (whether they have joined accidentally or have more nefarious motives). With new developments in video conferencing technology, including additional security measures and features being added as risks are developing in real time, providers now allow hosts to see the names and numbers of the participants that have joined the conference, have given hosts the ability to set passwords or require their approval before each individual can join the conference, and allow the host to lock the meeting to prevent new participants from joining. As we have seen the surge in so-called "Zoom-bombings" leading to the roll out of these additional features over the last few weeks, it is yet another great example of the importance of consistently deploying software updates to make sure you have all the latest protections.

Now that you have made sure the right people – and only the right people – are in the conference, it is also important to keep in mind what documents or programs you may have open on your computer so you do not inadvertently share sensitive information if you, intentionally or by accident, use the screen-sharing features that many of these platforms provide. In addition, do not forget to make sure any sensitive information (whether business or personal) on your desk or in the background is out of view of your webcam, and leave the meeting (or at least mute yourself and leave the room) if you have to answer an urgent call during the conference. Some video conferencing services even now provide chat features, the content of which does not just disappear once the meeting is over, so avoid transmitting any sensitive information that way as well.

Smart Devices and Webcams

Smart devices have made our lives more convenient than ever, but in order for them to do their jobs, they must constantly eavesdrop on our conversations. Unsurprisingly, they have the ability to transmit that information and are not immune to the threats of hackers. As a result, you should ensure that your smart devices are turned off when you are joining conference calls and any time that you and your family are discussing sensitive information. Similarly, we have all seen the horror stories in the news of webcams being activated remotely by hackers, so be cognizant of them when not in use and keep them covered.

Back to Basics

While you consider all of these innovations in technology and the new ways your sensitive information can get into the wrong hands, do not forget about Cybersecurity 101. As always, you should ensure that all of your devices and apps are protected with strong and unique passwords (this includes your home Wi-Fi and access to settings on your home router, which may be set to default passwords), and that you do not forget to log out of devices when they are not in use. In addition, avoid throwing away documents that may contain sensitive information, and, instead, make sure everything gets shredded first.

In the event that you become aware of a possible threat or – in an abundance of caution – think it is best to confirm that nothing untoward is going on, you should report anything suspicious to IT security specialists. If your family office does not have a dedicated IT security resource, your advisors can likely identify one for you, which will help make handling a cybersecurity incident that much less stressful. There is no foolproof way to completely insulate your family office (and your family) from these ever-evolving cybersecurity threats, but everyone involved can help minimize the risks, so stay vigilant and stay safe – because everyone involved can also open the door to an unwanted "cyber guest."

Contacts

Daniel G. Berick
Partner, Cleveland
T +1 216 479 8374
E daniel.berick@squirepb.com

Amy E. Gilbert
Associate, Cleveland
T +1 216 479 8732
E amy.gilbert@squirepb.com

The contents of this update are not intended to serve as legal advice related to individual situations or as legal opinions concerning such situations, nor should they be considered a substitute for taking legal advice.