The security expert’s tips on working outside the usual office environment

By Leif Nixon,
Security Expert at Sectra Communications

Working remotely brings greater freedom and flexibility to your workday. New opportunities arise when work can be conducted from any place at any time. The change from the stationary office to working remotely can lead to many positive effects, but it can also come with risks, meaning it is all the more important to protect sensitive information.

The ways in which we can work remotely have developed rapidly, but cybercrime has also risen alongside this. Poorly protected remote desktop servers and phishing e-mails are among the most common avenues of attack. These can both cause significant harm to the employee that is exposed and damage the entire organization. It is important to protect against risks such as these, while making sure that it is easy for employees to do the right thing.

If circumstances dictate that it is not possible to come in to the office, how can your organization support the workforce in working both safely and efficiently? Below are some tips to consider if work needs to be done remotely.

Mobile devices

The first question that your organization must address is: What kind of device(s) do employees require to be able to work remotely? All employees require some kind of remote device to be able to function in the same way as they would when at their stationary workplaces. A powerful stationary computer or perhaps a laptop may be required. Sometimes, work can be conducted on a tablet or a smartphone, perhaps connected to the workplace via a remote desktop. Different kinds of devices come with different opportunities and challenges that can be important to consider when choosing your security solution.

Tips

To reduce the risk of attacks, it is recommended that a tablet or smartphone communicating via a secure VPN is used, and that the VPN is automatically always running in the background. The reason that a VPN should always be activated is to ensure that you are never working unprotected. This can help you to avoid several of the risks that are described below.

Risks when using mobile devices

For obvious reasons, there is a greater risk that mobile devices can be lost compared to stationary computers, which means that they can be exposed to different types of risk.

Apps and other downloadable data

One of the greatest security risks comes with apps and data that have been downloaded to a device. These can contain harmful code that can allow eavesdropping on a device. This can mean, for example, that the microphone and/or camera is activated without the knowledge of the user, or that data is sent to unintended parties. Another significant risk is that the app manufacturer could collect information about your online behavior and subsequently sell this data to other parties.

Tips

You can minimize this risk by only allowing apps that have been reviewed from a security perspective using whitelisting and blacklisting policies. If it is important for a user to have greater ability to choose which applications and downloads they wish to have, it is possible to protect work-related information by assigning a specific workspace in the device that is separate from the personal part of the device.

User data storage

If information is stored in the device, it will become inaccessible to the user if the device is lost or stolen, and there is the risk that others will be able to access sensitive information.

Tips

With security policies that prevent the user from working with locally saved data, the risk of data falling into the wrong hands can be reduced. Encrypting the data stored on a device ensures that information and documents cannot be accessed or read by the wrong person. It is important to find the right balance of security, using encryption solutions, depending on the security threats that you have identified.

It is also important to consider whether the organization's employees should only be permitted to work against a central server, which can of course come with a certain lack of flexibility if the network service is unreliable, or if it is allowable to save information locally. The risk of locally stored information on a device falling into the wrong hands can mitigated by applying a remote wipe capability. On the other hand, information can also be lost to the intended audience if it is not also stored centrally.

Eavesdropping

Mobile devices typically connect to any previously used wireless network. With a laptop, it is often the user that manually selects which network to connect to. In both cases, the network is often only identified by a simple name label, without any underlying technical guarantee of the network's true identity. When a device is connected to a network that you are not in control of, you run the risk of eavesdropping or being exposed to a man-in-the-middle attack (MITM).

If you connect to an open Wi-Fi access point at, for example, a café, anyone in the surrounding area could eavesdrop on your traffic. An attacker could also trick your device into connecting to a malevolent access point that is masking as the café's Wi-Fi. The attacker could then eavesdrop and alter the traffic, regardless of whether the Wi-Fi access point is open or encrypted.

Why protect sensitive information?

The reason that organizations need to have a clear policy on how sensitive or classified information should be handled is that there are attackers who wish to access this information. If you work in critical infrastructure, such as civil authorities, water and energy supply, the transport industry or the financial sector to name just a few, it is not impossible that highly motivated attackers with considerable resources such as foreign powers will be interested in the information that your organization handles. This can be the case even if the information is not classified. This can make up a piece of the puzzle in determining the nation's ability to resist society-impacting attacks, such as disinformation or sabotage. If you work in high-tech sectors, industrial espionage is probably your largest threat.

Tips

By using an end-to-end VPN, you can safeguard your data ("data in motion") and encrypt/decrypt data that is sent and received, reducing the risk of both eavesdropping and MITM attacks. For a VPN to be able to work well in a mobile environment, it is necessary to handle roaming (switching between networks) in a satisfactory way so that the user does not experience uneven access or must repeatedly log in. This is done so that work can be conducted as efficiently as possible, while information is kept secure.

Easy to do the right thing

In conclusion, it should be mentioned that the most important thing is for the employees of your organization to feel secure when handling sensitive information at their remote workplace. To achieve this, it is important to review security procedures and policies related to security in connection with remote working. Clear security procedures and guidelines are crucial.

Sectra AB • communications@sectra.com • communications.sectra.com
This is a marketing material and may be changed at any time without prior notice.
Sectra will not be held liable for any errors or misconceptions herein.