REMOTE WORKING CHECKLIST

GUIDANCE FOR PUBLIC PRACTITIONERS

The Essential Checklist for Controlling Data in Home Based Accounting Teams

In a central office, accounting firms can exert strong control over how their team members manage sensitive client data. But when teams transition to a hybrid or work-from-home environment, much of that control gets lost and additional risks can arise.

Luckily, there are some simple policies, settings and tools that firms can deploy to significantly reduce their risks. In this document Practice Protect share their top 11 free and low-cost tips for doing this. But first it's important to understand…

What's The Risk With Work-From-Home Anyway?

While many accounting teams are discovering that working from home can be easier than they first thought, it does come with some additional risks. These arise because:

- Home IT environments tend to be a lot less secure than business IT environments.
- Home devices tend to have multiple users who may be downloading unsafe programs hidden in browser extensions, movies, software etc.
- Home computing practices tend to be less strict. For example, many people save passwords in browsers or keychains on their personal devices.

Each of these factors causes a "blending" of data between home and business use. This introduces risks for the business and your client data. Luckily, these risks are very easily and cheaply addressed. Here are our top 11 tips for doing this:

1. Ensure your team are aware of the risks best practices (Free)

A good place to start is sharing this document internally. One additional risk that teams should be aware of right now is the prevalence of COVID-19 phishing scams.

Cyber criminals are taking advantage of the COVID-19 situation to send emails and messages that trick people into clicking official-looking links to steal their data. We are seeing a lot of these at the moment, so extra vigilance is required.

To view the latest scams and receive updates sign up at https://www.scamwatch.gov.au/

2. Where possible, have staff use a dedicated business computer at home.

Home computers tend to harbour more cyber threats. These are relatively innocuous if all you're doing is watching Netflix and online shopping. However, they can become a serious risk if business data becomes exposed. Where practical, the best solution is a dedicated business machine for each team member.

3. Get every team member to run a malware scan on their home computer if used for business (Free or Low Cost)

If it is isn't immediately practical for team member to use a dedicated business machine, we recommend getting every team member to run a malware scan on their home computers with software such as Malwarebytes.

Malwarebytes works on a PC and Mac and comes with a 14 day free trial that allows a thorough scan to be run at no cost. You may be surprised what gremlins this uncovers. Recently we saw a home computer scan return 220 threats and viruses.

4. Download a separate browser for work use (Free)

If team members must use their home computer, download a separate browser for work use. For example, if you tend to use the Chrome browser at home, download Firefox or Brave for work.

Browsers themselves tend to be quite secure. It's browser plugins and extensions that can introduce threats. By using a separate work browser, you quarantine your browsing from home-use plugins.

Browser plugins and extensions from reputable organisations (e.g. Google) are safe but be wary of other extensions that may reset or control browser settings in the background to steal your data.

5. Never save business passwords on your personal computer, browsers or keychains (Free)

Never save business passwords on your personal computer, or indeed in any browsers or keychains. One risk is that these passwords will be captured by keylogging software. Another is that these methods may make your passwords available on any connected device.

6. Set Settings to clear out your Downloads Folder and Recycle Bin fortnightly (Free)

Over time, your downloads folder can accumulate a cache of sensitive client information. We recommend clearing out your downloads folder and recycle bin on a regular basis. An article on how you can set this up in less than 5 minutes is here. In a business setting, we recommend a 14 day clearout rule, but for home computers we suggest once daily.

7. Consider setting up a dedicated business internet connection for work (Low Cost)

The advantage of a dedicated business internet connection is two-fold. Firstly, it preserves bandwidth for business purposes such as video calls. Secondly, it cordons off your business internet traffic from home internet traffic.

One simple and low-cost option is to buy a pre-paid device from Telstra for $50 to $100. Then ALDImobile offers prepaid data on the Telstra network at very cheap rates that can be plugged in.

8. Install a firm-wide password management tool (Low Cost)

The above tips are all useful and important but there's really no way to ensure that all of them have been actioned across your whole firm. A tool like Practice Protect encrypts passwords and shields them from being captured by keyloggers, phishing attacks and other schemes.

9. Implement a Location Control Policy (Low Cost)

This is a setting that can be switched on centrally with certain password management tools, which will automatically restrict login attempts from overseas. Most cyber attacks originate from overseas and this is a useful policy to shut down much of the risk.

10. Lock out access by policy during unusual time periods (Low Cost)

Similarly, a useful policy is to lock out app access during unusual time periods (e.g. 10pm to 5pm) when you wouldn't expect team members to be logging in. This can be setup for both server and cloud based access with the correct tools.

11. Implement a Work From Home Policy (Free)

Implementing a formal Work From Home Policy is a crucial step. (If you don't have one, there is a free fill-in-the-blanks policy template here). A firm-wide policy not only sets expectations, but it also limits your liability in the event of a data breach.

While all the above tips will significantly reduce your risk, if data is breached while your team is working from home, the first thing an insurer will look for is evidence that the employee knew what to do in the first place. If you can't demonstrate that such guidance was in place, your insurance policy may be rendered useless.

Conclusion and Next Steps

For many firms, working from home is an emerging development that may prove to have many benefits. However, it's also important to cover off the risks, which you can do by:

1. Circulating this document firm-wide
2. Putting in place all our free suggestions
3. Considering our low-cost recommendations

To learn more about how you can secure your firm CPA Australia Members can request a call with Practice Protect to receive a free assessment of their Cyber Security here.