p.c. peripherals

Tech Opinion – March 11th 2020

How to work securely from home

Irish business are encouraging workers to work remotely due to Coronavirus. Here’s how to facilitate it securely, says Sophos.

10th March 2020

Many, if not most, organisations have already crossed the ‘working from home’, or at least the ‘working while on the road’ bridge.

If you are on the IT team, you are probably used to preparing laptops for staff to use remotely and setting up mobile phones with access to company data.

But global concerns over the current Coronavirus (Covid-19) outbreak, and the need to keep at-risk staff away from the office, means that lots of companies may soon and suddenly end up with lots more staff working from home and it is vital not to let the precautions intended to protect the physical health of your staff turn into a threat to their cybersecurity health at the same time.

Importantly, if you have a colleague who needs to work from home specifically to stay away from the office then you can no longer use the tried-and-tested approach of getting them to come in once to collect their new laptop and phone, and to receive the on-site training that you hope will make them a safer teleworker.

You may end up needing to set remote users up from scratch, entirely remotely, and that might be something you have not done a lot of in the past.

So here are our five tips for working from home safely.

1. Make sure it is easy for your users to get started

Look for security products that offer what is called a Self-Service Portal (SSP).

What you are looking for is a service to which a remote user can connect, perhaps with a brand-new laptop they ordered themselves, and set it up safely and easily without needing to hand it over to the IT department first.

Many SSPs also allow the user to choose between different levels of access, so they can safely connect up either a personal device (albeit with less access to fewer company systems than they would get with a dedicated device), or a device that will be used only for company work.

The three key things you want to be able to set up easily and correctly are: encryption, protection and patching.

- Encryption means making sure that full-device encryption is turned on and activated, which protects any data on the device if it gets stolen; protection means that you start off with known security software, such as anti-virus, configured in the way you want; and patching means making sure that the user gets as many security updates as possible automatically, so they do not get forgotten.
- Remember that if you do suffer a data breach, such as a lost laptop, you may well need to disclose the fact to the data protection regulator.
- If you want to be able to claim that you took the right precautions, and thus that the breach can be disregarded, you will need to produce evidence – the regulator will not just take your word for it!

2. Make sure your users can do what they need

If users genuinely cannot do their job without access to server X or to system Y, then there is no point in sending them off to work from home without access to X and Y.

Make sure you have got your chosen remote access solution working reliably first before expecting your users to adopt it.

If there are any differences between what they might be used to and what they are going to get, explain the difference clearly – for example, if the emails they receive on their phone will be stripped of attachments, do not leave them to find that out on their own.

They will not only be annoyed but will probably also try to make up their own tricks for bypassing the problem, such as asking colleagues to upload the files to private accounts instead.

If you are the user, try to be understanding if there are things you used to be able do in the office that you have to manage without at home.

3. Make sure you can see what your users are doing

Do not just leave your users to their own devices (literally or figuratively).

If you have set up automatic updating for them, make sure you also have a way to check that it is working, and be prepared to spend time online helping them fix things if they go wrong.

If their security software produces warnings that you know they will have seen, make sure you review those warnings too, and let your users know what they mean and what you expect them to do about any issues that may arise.

Do not patronise your users, because no one likes that; but do not leave them to fend for themselves, either – show them a bit of cybersecurity love and you are very likely to find that they repay it.

4. Make sure they have somewhere to report security issues

If you have not already, set up an easily remembered email address, such as security999 @ yourcompany DOT example, where users can report security issues quickly and easily.

Remember that a lot of cyberattacks succeed because the crooks try over and over again until one user makes an innocent mistake – so if the first person to see a new threat has somewhere to report it where they know they will not be judged or criticised (or, worse still, ignored), they will end up helping everyone else.

Teach your users – in fact, this goes for office-based staff as well as teleworkers – only to reach out to you for cybersecurity assistance by using the email address or phone number you gave them. (Consider snail-mailing them a card or a sticker with the details printed on it.)

If they never make contact using links or phone numbers supplied by email, then they are very much less likely to get scammed or phished.

5. Make sure you know about "shadow IT" solutions

Shadow IT is where non-IT staff find their own ways of solving technical problems, for convenience or speed.

If you have a bunch of colleagues who are used to working together in the office, but who end up flung apart and unable to meet up, it is quite likely that they might come up with their own ways of collaborating online – using tools they have never tried before.

Sometimes, you might even be happy for them to do this, if it is a cheap and happy way of boosting team dynamics.

For example, they might open an account with an online whiteboarding service – perhaps even one you trust perfectly well – on their own credit card and plan to claim it back later.

The first risk everyone thinks about in cases like this is, "What if they make a security blunder or leak data they shouldn't?"

But there is another problem that lots of companies forget about, namely: what if, instead of being a security disaster, it is a conspicuous success?

A temporary solution put in place to deal with a public health issue might turn into a vibrant and important part of the company's online presence.

So, make sure you know whose credit card it is charged to, and make sure you can get access to the account if the person who originally created it forgets the password, or cancels their card.

So-called ‘shadow IT’ is not just a risk if it goes wrong – it can turn into a complicated liability if it goes right.

Most of all…

Most of all, if you and your users suddenly need to get into teleworking, be prepared to meet each other halfway.

For example, if you are the user, and your IT team suddenly insists that you start using a password manager and 2FA (those second-factor log-in codes you have to type in every time) then just say “Sure,” even if you hate 2FA and have avoided it in your personal life because you find it inconvenient.

And if you are the sysadmin, do not ignore your users, even if they ask questions you think they should know the answer to by now, or if they ask for something you have already said ‘no’ to because it might very well be that they’re asking because you did not explain clearly the first time, or because the feature they need really is important to doing their job properly.

We are living in tricky times, so try not to let matters of public health cause the sort of friction that gets in the way of doing cybersecurity properly.