SECURITY, OFFICE 365

5 WAYS TO SECURE OFFICE 365, IN A DAY!

BY
SHAUN ADAMS

SECURE OFFICE 365

Like correctly programming the time on your VCR back in the day, you must secure Office 365. In this instance, however, the risk is a lot greater. Instead of not being able to configure the automatic recording of your favourite TV Show while you're away from home - you'll be leaving a gaping hole in your business' security. Guaranteeing your digital security and privacy has never been more important than it is today.

Office 365 is resting on a truly impressive marketing campaign coupled with a solid product. As a result, the general assumption with Office 365 is that it's an off the shelf product, one that can be used by multi-national giants and Mum and Dad operations alike. Although when speaking of the availability of the platform this is true, the reality is, effective security is not so simple.

Microsoft has done a fantastic job. Pivoting their own business to an entirely new model. Not only embracing Software as a Service (SaaS) but challenging the entire Technology industry to simply keep up!

There are holes in multiple areas. Even in a specific enterprise product like Office 365 E3. Provisions to secure Office 365 exist, but are either not set up, or are so well known to the 'bad guys', they offer almost no protection.

That said, how are companies to secure Office 365 in a single day?

1) PASSCODES AND PASSPHRASES, NOT PASSWORDS

Fostering a change within your business to use passcodes instead of passwords is a phenomenally effective way to instantly beef-up security.

One of the most common causes of password loss, second to phishing, is a brute force attack. This means an algorithm has guessed your password. Most business networks have a default password policy. By default, they're set to make sure your password is more than 7 characters - that's it. Meaning that your policy dictates that across your business bubble1 is as secure as 0rFt*fz - it's clearly not. Something to remember when speaking about security is the good guys have to win every time - the bad guys only need one win.

We'll cover more on this in an upcoming post.

2) ENSURE NO ACCIDENTAL SLIPS

A favourite of Qbt Consulting's is Data Loss Prevention or DLP. First seen in Microsoft Exchange Server 2013, it's a layer of coding that sits atop the entire Office 365 platform identifying, monitoring, and protecting sensitive information. It uses deep content analysis and a list of rules to 'ear-mark' documents that match conditions you've set. You can use DLP to ensure that documents containing sensitive information cannot leave your business. You can also add Policy Tips that show up if a rule has been triggered. This allows the person who triggered the rule to re-think their actions.

3) MULTI-FACTOR AUTHENTICATION

The security measure that we all love to hate. We love it because it works. Period. We hate it because let's face it, it's annoying. The principal of Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA) is similar to bank vaults in movies. No one method can unlock your business's information vaults. You can have someone's password, no matter how complicated it is. But without their mobile phone, or tablet, you've got zero chance of getting into the account. Some things to note before adding MFA to your business are:

TRAIN, EDUCATE, TEST, THEN TRAIN AGAIN

People lose phones. It happens. A strong password and a device is the only way this method can work. If your users lose their phones, they need to know how to register their replacement device. There's nothing worse than having your CEO in a different country calling you from a payphone after losing their iPhone AND access to their email.

BACKUP METHODS

In each layer of this protection method, you're able to set your rescue address and mobile number. In the event of losing access to either your password or device, these will save the day. Make sure your users know that these are now crucial to corporate security as well.

CREATE CONDITIONAL POLICIES

When implementing MFA, a keen technology partner (like Qbt Consulting) can assist you in the creation of special rules to govern it. These rules can stipulate that if you're in your office, or on a trusted computer, you will bypass MFA altogether.

4) ADVANCED THREAT PROTECTION (ATP)

The bad guys are getting smarter, sneakier and bolder. Malware is a silent killer. A study in 2016 found that the cost to Australian business as a result of malware infection soars right beyond $74 million. Built into advanced add-ons for the Office 365 product is one of their most impressive forms of defence. This ace in the hole is a Cloud-based email filtering solution that is surprisingly effective in blocking unknown malware, zero-day attacks and other malicious content. In addition to actually blocking the mail, as you can imagine, there's a robust reporting component. You're able to see, quite easily, what attacks are coming to your business. This will assist you in your future cyber-security planning.

5) HUMAN FIREWALL

Like I said above, the good guys have to win every time - the bad guys only need one win. More than ever, your users are the weak link in your network security. You can complete all the aforementioned steps to perfection. It just takes one user to click to have all your work undone and your network exposed for the world to see.

Your staff require expert knowledge, training and experience. One of the biggest mistakes we see almost constantly is our partners spend big on training programs, days, sessions that are objectively really good. They're concise, correct and have some great content. That's not the mistake that they make. A few days or weeks after the training, because security isn't being kept at the top of mind, they're just as susceptible as before!

As a direct result of this, Qbt Consulting has created the Cerberus: Awareness and Training Program. It combines world-class expert training material in bite-sized chunks (3-5 minute videos) with ongoing, random, realistic simulated phishing attacks. By subjecting your staff to this sort of training, you're ensuring that they keep security at the top of mind and start learning better habits when it comes to e-mail and business security.

So there we have it, 5 Ways to Secure Office 365, in a Day! If you have any questions or would like to talk to us about finding out how exposed your business is to phishing attacks and malware, please contact us today!