The RefTech Cyber Security Checklist

UPDATED NOVEMBER 2022

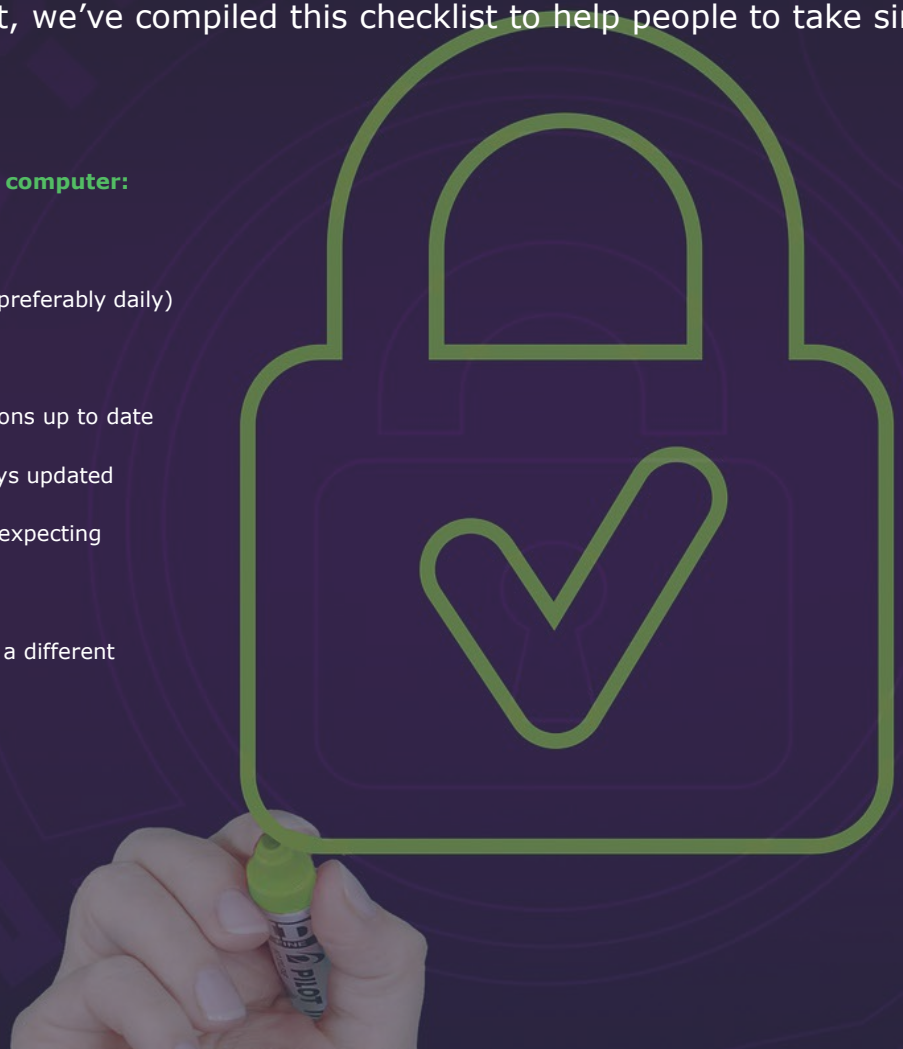
The events industry handles lots of personal data and it is important to keep that safe. We look at simple ways to help keep data more secure.

Cyber Security Checklist

We are constantly told of data breaches and cyber attacks in the news, so much so that it's easy to become a bit blasé about the whole subject – especially if it's not your field of expertise. The events industry handles a lot of personal data and it is important that we as an industry work to keep that personal data safe. To help with that, we've compiled this checklist to help people to take simple steps to become more secure.

Things you can do individually on your personal computer:

1. Backup all the data on your computer regularly (preferably daily)
2. Encrypt your computer's hard drive
3. Always keep your operating system and applications up to date
4. Have good anti-virus software installed and always updated
5. Never open an email attachment that you're not expecting
6. Be extremely wary of any web links in emails
7. Use a password manager to make sure you have a different password for everything
8. Make sure your passwords are strong
9. Know your most important passwords
10. Always use two factor authentication



1. Backup all the data on your computer regularly (preferably daily)

Before we get into more details for this one – a word of warning! **Don't** do this on your company computer without checking with your company IT team as to their preferred mechanism for backups. This is because some of these online services are located outside of the EU and that means potential legal problems if you are holding personal information on your computer.

However, on personal computers, this is number one for a reason. Computers (whether desktop or laptop) can and do fail or get lost or stolen and if your precious data/documents/photos/etc are only stored on your computer then you could be in real trouble if you can't get them back.

I also personally keep multiple backups of important files and folders and I do that with different backups in different ways. I use a Network Attached Storage (NAS) box at home which I backup to and I also have an online drive backup (think Google Drive, Microsoft OneDrive, iDrive.com and plenty of others have those) but USB drives are extremely affordable now and are worth considering if you don't have a NAS.

One of the best things about using an online backup tool is that you can install a small program on your computer to automatically back up your files when they change.

The downside to this is that if you are unfortunate enough to be hit by a ransomware attack where your files and folders are encrypted to try and extort money from you for their retrieval then you may find that the online versions are automatically updated.

That's why I keep a separate NAS drive backup that my computer backs up to without using a file share so those files would be protected in the event of an attack like that. Some online drive backups can do versioning of your files so you could go back to a previous version that wasn't encrypted but you need to check that out specifically with your chosen provider.

2. Encrypt your computer's hard drive

Again, this is a tip that you need to check with your IT team if you're looking to do this on your company computer. That said, encrypting your computer's hard drive is something you should really do as a matter of course. Encrypting your hard drive is very easy to do on either Windows or Mac and Googling will easily bring up current instructions for how do encrypt your drive on whatever operating system you're using.

The reason that encrypting your hard drive is a good idea is because there have been several incidents where an individual or an organization have been fined by the ICO after a computer holding personal data was stolen and where the data wasn't adequately protected. An encrypted hard drive would have provided that protection and avoided a fine.

3. Always keep your operating system and applications up to date

More than ever, this is a crucial step in protecting your computers. In 2022, Google announced several serious vulnerabilities in Chrome – the world's most popular web browser at the time of writing. A vulnerability is a bug in a piece of software that potentially allows an attacker to take over your computer and either spread to other machines or gain access to the data on the machine. Google have "patched" (meaning fixed) the bugs very quickly but there has been evidence that these bugs have been actively exploited. This means, if you're using Chrome and you see the "Update" word in the top right of the browser, click it as soon as you can!

However, it's not just Chrome that is affected, any software that connects to the internet can be vulnerable to attacks and should be kept up to date at all costs.

Cyber Security Checklist

4. Have good anti-virus software installed and always updated

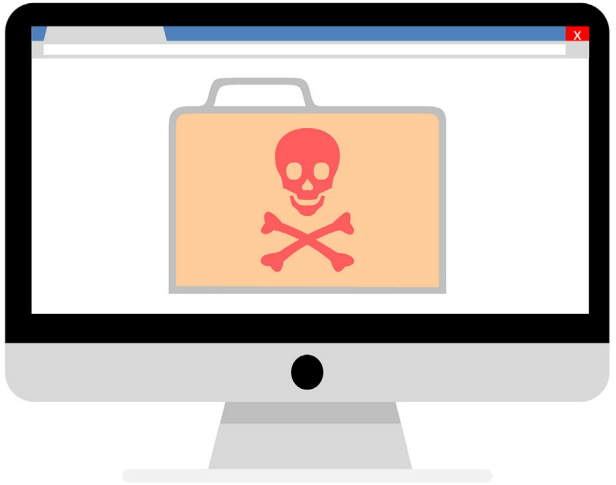
I won't get into a debate about which anti-virus is better than another here but having up to date anti-virus software running on your computer is essential. On Windows 10 and 11 Microsoft Defender is a good starting point for free but there are lots of other products on the market.

You need anti-virus software because there are so many threats around that it's hard to keep up with what dangers are out there. Some of our other tips are also related to this stuff. It's important to remember that these days there are organizations who are focused on trying to extort money from people by using "ransomware" attacks. These are attacks where your computer and possibly any other computers on a network with it can be encrypted if these gangs can trick you into opening a program that you shouldn't. The only way to get your computer and data decrypted is to pay their ransom.

It has been widely reported that these types of attacks are the most common threat in recent years because they're so lucrative. One US based travel organization reportedly paid $4.5 million in bitcoin to get their data decrypted after an attack. Of course, whether these gangs will ever give you the decryption key is anyone's guess!

As we said in the first point about having regular backups – if your backups are up to date then you should be able to restore everything from there rather than risk paying a ransom.

5. Never open an email attachment that you're not expecting



Once again, we're back to ransomware but other threats happen this way too. Attackers are getting better at writing convincing emails that look like they're from a genuine organization or someone you may know. This type of attack is known as phishing and has been extremely successful over the years. There's even an extremely targeted type of attack known as "whaling" because it goes after the biggest fish – the CEO of a company. In the worst known example of this type of attack, a CEO was tricked into having a large payment made to what he thought was a supplier. The fraudsters got away with $63 million and the CEO lost his job!

Don't be fooled into thinking that these type of attacks aren't aimed at everyone though – they absolutely are and most of the time they are in the form of an email with an attachment. The golden rule here is – if you get an email from someone you know with an attachment that you weren't expecting – contact the person using a method you know (i.e. don't just reply to the email) and ask if they really sent the email before you open it.

6. Be extremely wary of any web links in emails

In the same way that email attachments are dangerous, so are web links in emails. Again, it's normally criminals who want to trick you into either downloading a malicious bit of software or into revealing your login details for a site amongst other things.

It's fair to say the subject of phishing attacks is more complicated than it has ever been and there are plenty of huge articles just about this topic. The golden rule here is that if you receive an email asking you to login or with some alarming news and a link to login to prevent/permit said event – be extremely cautious.

Is the link from exactly the domain of the organization you think it should be? Misspelled domain names are a top target for malicious activity. At a quick glance pay-pal.com may look ok but the real domain doesn't have a hyphen. Equally, make sure there's nothing like paypal-security.com. If you're in any doubt – don't click the link but open your browser and go to the site yourself to see if there's anything wrong or contact the organization in question to ask if it's genuine.

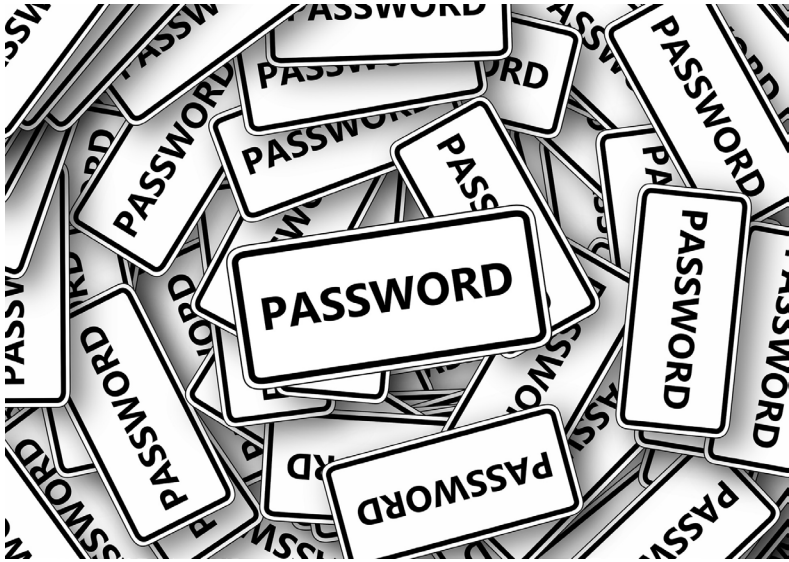
Cyber Security Checklist

7. Use a password manager to make sure you have a different password for everything

There are a lot of different Password managers these days and you can find lots of reviews of the top ones to help you decide which one you should be using but please make no mistake – you absolutely should be using a password manager.

The reasons for this are simple. Firstly, humans in general are terrible at password security which is why we see, year after year, lists of the most popular passwords discovered because of data breaches. "password" and "123456" will almost certainly be in the list next year as they were for the past umpteen years.

A password manager can help you with this by generating a secure password for every website, storing those securely and automatically filling them in when you go back to the website. Some people think that the password they use for everything is really secure so it won't be a problem but unfortunately, humans that create websites are also fallible and the other danger is that your password won't be stored securely and if they then get hacked then these passwords may be discoverable. If you are using the same password for more than one site then you leave yourself open to having more details stolen.



Check out https://haveibeenpwned.com/ to see what details of yours have been leaked – you might be surprised!

8. Make sure your passwords are strong

If you are using a password manager, then this step is a lot easier because most password managers can generate very strong and complicated passwords and store them for you.

However, if you aren't yet using a password manager then, at the very least, **I would implore you to ensure that you have a completely unique password on your email that is not used by ANY other system.**

This is because if an attacker can login to your email, then they can do pretty much anything as the vast majority of systems require you to receive an email as part of their password reset process.

If one of the many data breaches revealed the password you use for email and also included your email address then it's probably quite easy for an attacker to figure out how to login to your email and that is very, very bad!

9. Know your most important passwords

If you are using a password manager, then I would still recommend having two types of passwords. Ones that are stored in your password manager and ones that, as well as being stored in your password manager, you just know.

This is easier than you might think if you follow the advice in our free white paper https://www.eventreference.com/promo-www/passwords/download.php

The reason for this piece of advice is that your password manager will probably never let you down, but you can be absolutely sure that if it ever did, it'll be just at the moment when you need to login to your email and that's the time when your email provider will insist on you entering your password again!

Is the link from exactly the domain of the organization you think it should be? Misspelled domain names are a top target for malicious activity. At a quick glance pay-pal.com may look ok but the real domain doesn't have a hyphen. Equally, make sure there's nothing like paypal-security.com. If you're in any doubt – don't click the link but open your browser and go to the site yourself to see if there's anything wrong or contact the organization in question to ask if it's genuine.

Cyber Security Checklist

10. Always use two factor authentication

Two factor authentication (or 2FA) is a mechanism whereby you login normally with your username and password but then have to provide another piece of information which typically generated by a mobile app such as Google Authenticator. This piece of information often a 6-digit number and is time sensitive meaning it changes frequently, normally every 30 seconds.

That means even if someone were able to get your username and password, they would have to know how to configure this extra mobile app to give them the correct 6 digit "token" to be able to login to your account.

That adds a huge amount of security to your login credentials making it almost impossible to login as long as you're careful with the 2FA information. A huge amount of platforms have 2FA now and it is always worth enabling them if you can but make sure you know how you can access them if you can't get the 2FA token.

For more information on data protection, please download RefTech's free white paper titled: 'Data Protection in the Events Industry: what you need to know to stay within the law'
https://www.eventreference.com/promo-www/datasafety/download.php

+44 (0)1827 61666

sales@reftech.com

www.reftech.com

YOUR EVENT. OUR SERVICE.

Full badging & registration solution