
CYBER SECURITY
AT HOME

Table of Contents

How to Use Smart Devices in a Safe Way

Smart devices have really helped to make our lives so much more convenient. However, they can also pose a significant safety threat.

Whether you are using a smartphone or smart home products, as they are connected to the internet, they remain vulnerable to hackers. So, how can you make sure you use these smart devices safely?

Below, we'll look at some of the best smart device safety tips you can follow.

Strengthening Your Wi-Fi Security

As the main threat to smart devices comes through the internet, it's advisable to check your Wi-Fi connection. Ideally, you'll want to make sure your Wi-Fi has a strong encryption method, such as WPA2. It's also a good idea to change the name of your router. Give it a random name not associated with your address.

Another way to make your Wi-Fi more secure is to create a guest network. That way, if friends and family come around, they can connect to the guest network. Finally, you'll want to secure the Wi-Fi with a strong password, as well as change the default name of the network.

Keep Devices Locked with a Passcode

Any smart devices you use should be kept secure with a passcode. You may also want to consider utilizing the face ID locking feature many devices have these days. With this feature, the smart device only unlocks through facial recognition.

When setting a passcode, make sure it's something nobody else can guess. Avoid memorable dates such as birthdays and anniversaries as these can be easy for hackers to guess.

Don't Click on Any Suspicious Links

Criminals don't just gain access to your devices by directly hacking into them. They can also trick you into letting them in. There is a substantial number of phishing scams out there, supplying harmful links for you to click on.

These scams will usually ask you to confirm your account or change your password. Upon following the link and typing in your details, the hackers will have everything they need to steal your information. So, it's important to never click on links provided in emails and text messages unless you know and trust the sender.

Keep Security Software Updated

Anti-virus protection and VPNs are great ways to keep your devices safe. However, they need to be regularly updated. This is because hackers and fraudsters are continuously finding ways around existing security measures. So, security software needs to be also constantly updated to deal with the latest threats.

If your software hasn't been updated in a while, now is the time to get it up to date.

Tweak Their Privacy Settings

All smart devices come with some form of privacy. However, these aren't always switched on. So, take a minute to go into the privacy settings of the devices, seeing if there is anything that needs to be tweaked.

Keeping your devices secure is important in today's digital world. There are constant cybersecurity threats you need to be aware of. As our homes become smarter, we need to take extra precautions to deter criminals from accessing them.

What Do Companies Do with the Data They Collect From You?

Have you ever wondered what companies do with the data they collect from you? While stricter data laws continue to be introduced, it is a good idea to learn more about how your data is used.

Here, we'll look at what companies do with your data and the main things you need to know.

Assess Your Location

One of the main things companies do with the data they collect, is use it to assess your location. This even applies when you turn off GPS location tracking. They can track your location in a number of ways, including through your IP address.

While they claim the data is still anonymous, it can be worrying knowing your location is being tracked. Mostly, companies use this information for better targeted ads and services. For example, location data is used to supply information on local businesses.

Sharing Data with Affiliates

While laws are getting stricter over how data can be shared, it doesn't stop companies selling information to third parties. This can be done for a number of reasons. For the company selling your data, it's purely for monetary benefit. However, for the people collecting the information, it's to help them with their marketing.

You'll often notice that when you're asked to agree to terms and conditions on apps and websites, it states your information may be passed on to third parties. So, pay attention the next time you are presented with a data collection notice and see how your information will be used.

Advertising

By far the most common thing companies do with your data is to use it for advertising purposes. They collect data to give them a better understanding of their target market and the popularity of the products and services they offer.

Once they have the data, they can use it to better target their audience. They can make improvements to their products and services if needed too. So, mostly the data collected about you is used in a safe, uncompromising way. However, there are risks that come with sharing data that you should always be aware of.

The Risks of Sharing Data

Although there are specific laws relating to how data can be stored and shared, there are still risks you need to be aware of. Criminals are constantly looking to get their hands on consumer data. So, there is a risk your information could be sold to the wrong people. This is a very low risk, but it's still something to be aware of.

Some types of data can also pose a risk of revealing your identity. Location data can be easy enough to track, potentially giving away where you go each day and where your primary residence is.

Overall, companies collect a lot of different data from their customers and website visitors. Most of the time it is innocently used for marketing purposes. However, the way in which data can be used does pose some security risks you should absolutely be aware of.

How to Tell if a Website is Fake

There are hundreds of thousands of websites online and not all of them can be trusted. Some are designed with malicious intent, there to steal your personal information.

Shopping or browsing through a fake website can pose a lot of security issues. So, how exactly can you spot a fake website? Here are some of the main things to look for.

Look Closely at the Address Bar

One of the easiest ways to spot a fake website is by taking a look at its address bar. Some have top brand names included in the site, but there are a few giveaways that they aren't official.

The first thing you should look for is the http:// section. Secure websites will be written as https://. So, if the website doesn't have the "s" included, it isn't fully secure. Also, watch out for shopping sites which have an address that ends with .org or .net. These are very rarely used by retailers so it's an indicator you're dealing with a fraudulent organization.

Is the Product or Price Too Good to Be True?

Another sign the website is fake is if the price seems too good to be true. Research the average cost of the product or service it is advertising. Is the cost on the site much lower than it should be? If so, it's a sign you're about to give your payment details to a fake site.

Pay Attention to the Content

You can typically tell from the content of the website whether or not it is fake. Pay attention to any spelling and grammar errors. Does the website appear to be written by someone with poor English skills? While some businesses simply pay for cheaper content, others have been set up by fraudsters in non-native English-speaking countries.

You'll also notice there isn't much in the way of an About or Contact section. All reliable businesses will have a clear About Us page, telling you when the company was formed. They will also provide you with multiple ways to get in touch. So, if the website you are visiting has very little information, it's worth avoiding it.

Check Out Customer Reviews

A good indicator of whether a website is genuine or not, is by looking at its online reviews. All genuine businesses and websites are reviewed online so if you can't find anything about it, it is a clear red flag.

Don't just rely on testimonials provided on the website itself. Head to trusted review sites and search there. It's often easy to spot a fake website by simply checking for reviews first.

These are some of the best ways you can spot a fake website as you browse the internet. While visiting one may not necessarily cause any issues, filling out information and making a purchase via one can land you in serious financial trouble.

If you want to avoid falling victim to fake websites, it's extremely important to know how to spot them.

Creating a Strong Password

Sick of trying to figure out your online passwords? Whichever sites you try and register with these days, you're practically always met with, "be sure to use a strong password". The trouble is, you can't use anything that would be easy to guess. Ultimately, you create a random password, forget it and then have to start the process all over again.

What should be a simple task can be absolutely infuriating. So, how can you create a strong password and remember it? Here, you'll discover some great tips you can follow.

What Is a Strong Password?

First, let's look at what a strong password actually is. While the requirements vary between sites, you typically need to:

- Ensure you use a minimum character count
- Use a combination of letters and numbers
- Have at least one capital letter
- Use a special character

Not all sites require you to use a special character, but it's worth adding one in so you can use the same password for multiple sites. But wait, isn't using the same password for everything advised against? Well, it generally is, but using the same password helps you to remember it. The trick is to change the password frequently.

Tips for Creating a Strong Memorable Password

So, now you know what a strong password generally is, how can you create one you remember? The good news is there are lots of techniques you can follow.

Some experts recommend coming up with three or four random words and combining them together. That could be four words that mean something to you. Then, make sure the first letter of the password is capitalized and add a couple of numbers at the end. It would look something like this:

Thebeetlethatflew57

You can choose any four words you like. Many people find this an effective way to remember their strong passwords so it's definitely worth trying.

Generally speaking, the longer you make your password, the harder it will be for fraudsters to hack. Try to create a password that contains no fewer than 15 characters.

Use a mixture of characters too and avoid keeping a copy of your password on your computer.

The main thing to remember is to avoid using anything too obvious. Don't use the word "password" for example and avoid using your date of birth.

Take Advantage of Password Managers

If you still struggle to remember your passwords, it might be time to use a password manager. These store and remember your passwords for you and there are a lot of them out there. Make sure you're choosing a reliable, trustworthy password manager, however. There are a lot of fake ones around so always use one by a brand you trust.

Creating a strong password that you remember doesn't have to be overly difficult. The above are just some of the great tips you can follow. Ideally, you'll want to change your password every few months too. This will make it really difficult for hackers to keep up.

MITM Attacks – Protect Yourself

There are a lot of types of cyber security attacks out there and MITM is one of the most common. Known as a Man-In-The-Middle attack, there are different types to be aware of and each poses its own issues.

So, what exactly is an MITM attack and how can you prevent them? Read on to find out.

What Is an MITM Attack?

An MITM attack is where a fraudster places themselves between a computer and server. From there, they can basically eavesdrop on what is being shared. Some attackers can also modify the information.

One of the stand-out features of an MITM attack is that you don't even know it's happening. It's also worth being aware that there are different types of MITM attacks you can fall victim to.

The Different Types of Attacks

An MITM attack can occur in different ways. The most common types include:

- IP spoofing
- HTTPS spoofing
- Email hijacking
- Wi-Fi eavesdropping

Your IP address is a number that has been assigned to your device depending upon your location. Hackers can spoof an IP address, making it appear as though you are interacting with a website or person you are trying to communicate with. They can also do the same with HTPPS addresses. They make small tweaks to the address, such as using lower case letters where capitals should be, etc.

Email hijacking is also common, involving victims being sent spoof emails. These are often addressed from banks or other leading organizations. They tell you to provide personal information which they will then use to log in to your bank account.

Finally, Wi-Fi eavesdropping aims to steal information about a victim's internet activity. With this type of attack, the fraudster actually creates their own internet hotspot. As soon as someone connects, they can then monitor which sites are used, as well as capture login information.

These are some of the most important types of MITM attacks you need to be aware of.

How Do They Work?

The majority of MITM attacks occur through public networks. This is because these are much easier to hack. The attacker needs to compromise the router. This is typically done by using tools to scan for vulnerabilities and flaws. They then need to intercept as well as decrypt the transmitted data. This part can be done using a wide variety of techniques such as packet injections, sniffing and session hijacking.

It's worth researching each of these techniques so you can have a better understanding of how they all work.

Now that we've covered what an MITM attack is and a basic idea of how they work, how can you defend yourself against these attacks? The simple answer is to avoid public networks. However, you can also use a VPN, make sure you're only visiting legitimate websites and avoid clicking on any links from anyone you don't fully trust.

MITM attacks are common and they can be tricky to spot. The above are just some of the main things you should know about these attacks in order to defend yourself.

Scams on Social Media

Social media has become deeply ingrained in our daily lives. While it can be an invaluable platform for keeping in touch with friends and family, it also poses some pretty big security risks.

There are a lot of scams operating through social media channels. Whether you use Facebook, Twitter or Instagram, it's important to be aware of the scams in circulation so you can avoid falling victim to them.

Here, we'll look at how social media scams work and how you can potentially spot them.

What Types of Social Media Scams Are There?

There are a surprising number of social media scams out there. The main ones include:

- Fake friends
- Fake ads
- Free app downloads
- Hidden URLs
- Quizzes

Fake friends and ads are particularly common. With fake friends, you'll have people you don't know asking to connect with you. They are usually using fake photos and information and their goal is to get money out of their victims. They usually build up a friendship over time before asking for money for some kind of emergency.

Fake ads are in abundance on social media. They advertise a variety of products but fail to send them after payment has been made. Or, the items sent are nothing like what is advertised.

There are also apps you can download which are packed full of malware. A particular problem for Twitter users is hidden URLs. These are shortened links which don't show you the address of the website. While most do take you to a genuine site, others are loaded with malware.

Finally, online quizzes are really popular with social media users and attackers take advantage of this. The information you supply through these quizzes is often stored and sold on to third parties.

So, there are a lot of scams to be aware of on social media. The question is, how can you sport them?

How to Spot Social Media Scams

While social media scams are rife, there are some easy ways to spot them. In terms of fake friends, simply avoiding adding anybody you don't know is the best advice you can follow.

If an existing friend suddenly tries to add you with another account, you should also be wary. Fraudsters are starting to create profiles of friends and family, making it look like

you know the person adding you. They then quickly ask you for money. In fact, if anybody asks you for money on social media, it's most likely a scam.

Another tell-tale sign is if the price of a product sounds too goo to be true. Anything in life that sounds too good to be true usually is. And finally, avoiding clicking on links and taking quizzes on social media will also lower your risk.

You can't always easily detect social media scams. However, being aware of what they are and how they work can help you to better protect yourself.

Anti-Viruses

As computer and smart device operating systems continue to become more secure, many question whether they actually need additional protection. The simple answer here is yes.

Although operating systems like Windows 10 are more secure, they are not capable of protecting you against every threat. Fraudsters and cyber criminals are becoming increasingly smarter. So, you will need to continually invest in the latest software to keep your account secure.

The question is, how much virus protection do you need? Read on to find out what you need to know to ensure you have the right level of protection.

Are You Using the Device for Work or Leisure?

When trying to decide how much virus protection you're going to need, it helps to consider whether you are using your computer for work or leisure. While protection is important in either case, the level of protection you need will differ.

If you're using your computer for work for example, it's vital you keep your business details secure. Fraudsters target businesses much more forcefully than personal users. So, you're going to need a high-quality anti-virus program to protect a business system.

With computers that are only used for leisure purposes, you could potentially get away with using free virus protection software.

Utilizing Free Tools

There are a lot of free tools you can use to keep your computer protected. Windows comes with its own secure tool known as Windows Defender. In many cases, this could be enough security for personal computers. However, it doesn't hurt to install more free protection.

Take a look online and you'll find a huge range of free anti-virus software tools out there. Some of the best ones to consider include:

- Avira
- Sophos
- Panda
- Kaspersky

These are just a small selection of the free anti-virus tools you can use. While they won't detect every single threat, they will protect you against the majority. Read as many reviews as you can as these will help you to determine which free solutions work better.

Focus on More Than Virus Protection

It isn't just virus protection you need to worry about in terms of cyber security. Having good anti-virus software is the first step to keeping your system secure. However, you'll also want to look at malware protection and VPN security.

Most modern anti-virus solutions also include malware protection. However, you may want to look out specifically for malware protection tools. Signing up to a VPN is also recommended as this shields your IP address. It helps to keep your system away from prying eyes.

Another thing to factor in is phishing. Anti-virus software won't always protect you against phishing scams. These are typically emails with links that lead you to enter your information. The fraudsters then steal that information. So, avoid clicking on any links that haven't come from a trusted source.

So, if you're wondering how much virus protection you need, the answer is that it depends. However, the general takeaway should be that the more security you have, the better. While free programs are extremely useful, it is much better to invest in a paid anti-virus solution. These come with a lot more features and added protection.

2021 Cyber Security

If you want to stay on top of cyber security, it's worth keeping an eye on upcoming trends. As attackers become more sophisticated, so too do our security solutions. So, what cyber security trends should you look out for in 2021?

Multifactor Authentication

Multifactor authentication is nothing new, but it is set to become more prevalent in 2021. It basically provides additional protection by asking you to verify your identity.

After typing in your username and password, you will be sent an additional code to type in. This is an additional user verification step and prevents hackers from gaining access to your information. Even if they guess your username and password, they won't be able to access your account without going through the additional security check. As a code is usually sent to your mobile number, only you will have access to it.

Data Protection

The amount of data that businesses create and store increases with each passing year. Unfortunately, hackers are constantly looking at ways to get their hands on this data. That's where data protection comes in.

In 2021, there is going to be a lot more focus on data protection techniques – making sure you store your data on a secure platform, as well as preparing for all kinds of threats such as cyber-attacks, human error and file corruption.

5G Security

5G technology is set to hit the mainstream next year. While it has the potential to dramatically boost internet speeds and boost reliability, it also poses a lot of security questions.

Hackers are already going to be looking at ways to compromise 5G systems. So, there is a need for strict 5G security software and techniques to protect users against the potentially complex risks.

Cyber Insurance

As cybersecurity issues become more prevalent, cyber insurance is set to dominate the market. Providing protection in the event a business is compromised, this type of insurance will be considered crucial.

Like any type of insurance, it is important to compare providers. Not all policies will include everything you need. So, you'll want to make sure the insurance you are investing in covers the potential risks you are exposed to.

Filling the Cyber Security Skills Gap

At the moment, there is a shortage in cyber security skills. From 2021, we can expect to see more people enter the sector, filling the gap for better protection. Cyber security experts will prove invaluable at protecting both consumers and businesses from cyber-attacks.

As you can see, there are some exciting cyber security trends in 2021 to watch out for. As technology continues to advance, so too does cyber security. As the recent

pandemic has forced many of us to start working from home, online security has become a major factor.

It is more crucial now than ever before to protect ourselves and our data from attackers. So, throughout the year ahead, we are sure to see a lot more cyber security tools and software introduced onto the market.

Touch Screen Devices and Their Security

How safe are your touch screen devices? When we think of protecting our devices from security threats, it is common to focus on software. However, as software-related hacks are becoming increasingly difficult, hackers are looking into new ways to get into your systems.

Nowadays, the components of smart devices are frequently being targeted, including the touch screen of phones and tablets. So, how can you protect your touch screens against the potential threats they are exposed to?

Here, you'll discover the key things you need to know about cyber security and touch screens.

What Threats are Touch Screens Up Against?

There are a few threats touch screen devices are vulnerable against. The main ones include keylogger and tap 'n ghost attacks.

Keylogger attacks are extremely complex, which means that they aren't overly common. However, it is still worth being aware of the risks they present. This type of attack relies upon the hacker capturing where the screen is touched and taking a screenshot from the device to see what the user is typing. With keylogger attacks, applications are typically running in the background of the operating system. They are able to record everything the user presses, including touch ID details.

Tap 'n ghost attacks also rely upon a two-step method. The attacker will prompt the user to accept a connection to a Bluetooth device, for example. Even if the user clicks cancel, a connection is established, giving the attacker access to the system. Once they do have access, they can actually control the device, pairing it with another one or simply stealing its information.

These are the main types of threats that exist for touch screen devices. Both are extremely complex, which means they are thankfully uncommon.

Why Are Touch Screens a Security Risk?

You don’t typically associate security risks with touch screens. However, they can capture unique personal information such as IDs, passwords and usernames. Therefore, regardless of how they connect to a device, they have the potential to be compromised.

Software can be protected with a certification code, whereas a touch screen doesn’t have this option. It isn’t possible to determine whether electronic hardware has been tampered with. Hidden radio transceivers for example, could easily be placed behind a touch screen.

So, the fact touch screens aren’t as easy to protect against cybersecurity threats makes them an ideal target for criminals.

How Can You Protect Your Touch Screen Device?

Making sure you buy your touch screen devices from a reliable source is the first way to protect yourself. Buying a brand-new device rather than a refurbished one will reduce the likelihood your device has been tampered with. You should also be careful where you leave your device and who repairs it.

Thankfully, touch screen-related cyber attacks aren’t overly common. However, it is something you should be aware of, particularly when it comes time to repair the device. While there isn’t much you can do to protect yourself from these attacks, following the advice above can really help.

Cloud Do’s and Don’ts

The cloud has drastically improved the way businesses and consumers store and manage important files. Eliminating the need for physical storage, it can save a significant amount of space on your hard drive.

However, while the cloud does offer a lot of benefits, it can also pose significant security threats. If you plan on using the cloud for work or leisure, below you’ll discover some security do’s and don’ts you should absolutely follow.

Do Consider Paying for Private Cloud Access

There are two variations of the cloud. One is free and the other one offers paid access. So, what’s the difference? Well, the free version is a public cloud, whereas the paid subscriptions give you private access.

The free version is often recommended to most users. However, even if you’re only using the cloud for personal rather than business use, it could still be worth paying for

private access. This is much more secure and keeps your personal information away from prying eyes.

Don’t Just Sign Up to the First Provider You Find

There are a lot of cloud providers out there and no two are the same. Therefore, you’ll want to avoid simply signing up to the first provider you come across.

Do your research to see what each provider offers. Take a look at online reviews to see what others have to say. These often reveal how easy to use the platform is, whether it’s worthwhile and whether there are any downsides you need to be aware of.

Comparing providers will ensure you make the best choice to match your storage needs. Most importantly, you should look to see who else will have access to the things you store and how data can be retrieved.

Do Look at the Security Options Provided

Even with the paid cloud subscriptions, the level of security provided can differ. The best ones to go with are those which utilize several layers of protection. There are also providers who require credential verification between your data and access point.

The more security the cloud provider supplies, the safer your information and files will be.

Don’t Move Everything to the Cloud

Finally, while the cloud does offer convenient storage, it is important not to use it for everything. Make sure some information is stored away from the cloud just in case the worst does happen and a hacker gains access to your files.

Not everything can be moved to the cloud anyway. Some applications need to be extensively modified before they are able to be incorporated there. So, don’t see it as an all-in-one storage solution.

These are some of the most important dos and don’ts when looking into cloud security. While the cloud is mostly secure, there are different levels of protection out there. Therefore, it’s important to compare your options and ensure you are choosing a reliable provider. You should also make sure your passwords are secure and difficult to hack.

BONUS – Social Media Posts

1. **How to Make Your Password Strong and Still Remember It**

Post: Creating a strong, memorable password isn’t easy. Our new blog reveals some great tips you can follow. LINK

2. **How Much Virus Protection Do You Need?**

   Post: Wondering how much virus protection you actually need? Generally speaking, the more you have, the better protected you will be. Learn more here. LINK

3. **What Companies Do with Your Data**

   Post: Companies can use your data in a variety of ways. Find out more in our new blog. LINK

4. **Tips for Using Smart Devices Safely**

   Post: Smart devices can pose a security risk. That’s why it is so important to keep them protected. Here are some great tips you can use. LINK

5. **Cyber Security and Touch Screens**

   Post: Did you know your touch screen device could pose security issues? Read this to find out more. LINK

6. **Cloud Security Do's and Don'ts**

   Post: When investing in cloud computing, it’s worth paying for private cloud access. Read this new article for more cloud security tips. LINK

7. **How Social Media Scams Work and How to Spot Them**

   Post: There are so many social media scams you can fall victim to. From fake friends and advertisements to malware loaded quizzes; learn how to protect yourself today. LINK

8. **How to Spot a Fake Website**

   Post: Taking a look at the content of a website can help you to determine whether or not it is fake. Learn more here. LINK

9. **How to Defend Yourself from MITM Attacks**

   Post: An MITM attack isn't always easy to spot. Here's some ways to keep yourself protected. LINK

10. **Cyber Security Trends in 2021**

    Post: Check out these top cyber security trends to watch out for in 2021. LINK