Computer Club

iPad Security

October 2021

As with all computer security matters, there is a level of detail and complexity that many average users will struggle to follow. This topic is no different so just feel free to ignore that stuff you can't understand but make a real effort to understand the Blue Text. This is the information you need to know to achieve a reasonable level of security when online. If there is some aspect of this that you don't understand, please make a point of asking for a bit more of an explanation

Definitions:

Malware – An umbrella term for all kinds of unpleasant internet things designed to get your information and or money

Virus: A piece of computer software often hidden in something that looks safe, designed to run and interfere with your computer system or gather private information to get money from you or make money from information extracted from you.

Jailbreak: Modify your iPad to allow Apps to be downloaded from sources other than the App Store.

Phishing: Web sites/ emails/ messages Designed to appear like the real thing such as 'The Royal Mail' but are designed to deceive you and encourage you to click on links and enter your data

Fake Ads: Book a Villa online in Spain from a company that do not own the apartment and are not authorized to rent it out.

Ransomware: Threats received that all of your data will be destroyed if you don't make a payment. You cant access any of your stuff when the threat is received

Pwning: Receiving a blackmail email threatening to release information about you using your hacked data or similar unless you pay money, often provides evidence of your password to show that you have been hacked.

This is a Link: When you click on a link it typically takes you to a website giving you more information on a topic. When a web page loads in your browser it can be designed to run code in the background that may be harmful. Click this link to demonstrate.(This is a safe link)

<div align="center">

Computer Club
iPad Security
October 2021

</div>

Do I need Anti Virus Software on my iPad?

You do on Android Tablets and Phones, You do on a Mac or Windows Computer but not on an iPad. One of the main reasons for this is that the Apps that you use all come from the Apple App Store. They are tested and designed so that a virus can't be included within the App and extend itself into the rest of your system

BUT things like Fake Ads, Phishing Scams, email attachments, downloaded files and some other Malware can get through so read on to learn more.

If you Jailbreak your iPad – Ignore the above comments as you will be at risk from all manner of Malware because the Apps that you may download may not be safe.

What is Adware

Adware creates targeted Ads by tracking you online. It's common to see oddly targeted Ads when browsing the internet for things we may have searched for.

If you think you may have adware:-
- Open Settings
- Open Safari (follow similar steps for whatever browser you favour)
- Clear History and Website data. Your Web History and Cache will be cleared.

  Read on for more information about Browser security settings

What is Spyware?

This can be hard to spot and you won't see the effects of it as it gathers your data and tracks your online activity. It may even disguise itself as legitimate software(A Trojan)

Where does it come from? Whenever you download files and save them to your iPad or click on a link in an email attachment unless you know that these sources are totally safe, you are at risk.

The risk is relatively small but as you can see below, there is no guarantee that your iPad would be immune.

Computer Club

iPad Security

October 2021

13th September 2021
Apple has released an urgent security update for Mac, iPhone, iPad and Watch users
after researchers discovered a zero-day, zero-click exploit from a spyware company that gives
attackers full access to a device's camera, microphone, messages, texts, emails, calls and more.

It's more difficult to spot on the iPad than the iPhone. The iPad may receive unusual messages, your phone may start to consume more data than you expect. Your phone battery may run hot when you are not running apps. Other peculiar behaviour that you can't explain.

Adware and Spyware are very rare on the iPad most malicious emails and downloads are written for different systems but it's not impossible as referenced above.

Phishing is a more common problem

Consider this scenario

You receive an email from what appears to be your bank telling you of a problem and providing a link in an email that you are asked to Click for Help

You click the link and what appears to be your bank's website opens asking you to log in and then take some kind of actions

THIS IS A PHISHING ATTACK sometimes supported or initiated by a telephone call

More examples - Royal Mail message saying you owe a small sum on an undelivered package
Royal Mail message with a tracking link without any reference to the original purchase

Other examples

- It references 'suspicious activity' on your account or 'login issues'
- Claims there is a 'problem with payment information on your account'
- Tells you to confirm some personal information
- Perhaps includes a fake invoice.
- Asks you to click a link to make a payment
- Says you are eligible for a refund or similar
- Road Tax scams
- HMRC scams

iPad Security

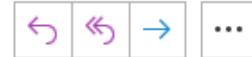October 2021

Here is an example of a fraudulent email

Fwd: Note ffrom Peter Brindley

PB Peter Brindley <ahmedshingaly@cau.ac.kr>
To all
Fri 22/10

(i) Follow up. Start by 26 October 2021. Due by 26 October 2021.

On Friday, October 22, 2021 10:46 AM, Peter wrote:
Just wanted to ask you if you may remember the guys in this photograph:
https://emea01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.gndm.aoefpna.com%2F&data=04%7C01%7C%7C6be89c18430441c3d30308d9957ee920%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637705194570225113%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=U2zcawjpR4WadpSz8mpKRSNWuq%2Bn3DTznzFWTQKtxpg%3D&reserved=0

1. It's from one of my Contacts – Peter Brindley
2. Note the spelling error in 'ffrom'
3. I don't normally get emails from him though we are friendly.
4. Look at the email address it came from – 'ahmedshingaly' It's obviously bogus
5. The text is a typical short invitation to click on a link
6. If I click on the link I don't know what the consequences would be, probably nothing lasting but you never know.
7. It could just as easily say 'Here is your invoice attached'
8. If I hover my pointer over a link I can usually see where it will take me.

iPad Security

October 2021

Here are some guidelines for recognizing and avoiding these scams

- Always be suspicious of any email that you receive asking you to do something. Especially if unexpected. Your first thought should be, is this a scam!
- Never click on a link provided in an email to take you to a website especially for financial transactions. Always use your usual method of going to the website. If in doubt ring up the company but don't use the phone number from an email.
- Look for clues on a website or in an email such as spelling errors or email addresses that are plainly not from the, so called, sender
- Do open attachments in emails unless you totally trust the source. Do not think that because the email seems to be from a contact, that they sent it to you. Emails with short messages like 'saw this and thought you would like it referring to attachments or links. THIS IS COMMON.
- Never trust alarming messages
- Enable MultiFactor authentication

IF YOU THINK THAT YOU HAVE LOADED A FAKE WEBSITE, CLOSE THE BROWSER, CLEAR THE CACHE AND HISTORY POWER DOWN THE IPAD AND RESTART

Safari Privacy Settings

Go to Settings >Safari

Block popups – Yes

Prevent Cross-Site Tracking – Yes

Hide IP Address from Trackers – Yes

Block Cookies = No

Save details for autofill on Forms but perhaps not Credit Cards

Fraudulent Website Warning – Yes

Privacy-Preserving Ad Measurement – Off

Allow a check for Apple Pay = OK if you use it

Clear History and Website date = Do it when needed

Safari is optimized for use with the iPad. It incorporates features that help to protect your privacy and security. It works with Keychain, the Apple Password Manager and features many settings to improve your control over your information.

Chrome is a very popular browser but there are very few settings to allow the same degree of control as Safari provides. Keychain does not work with Chrome. If you need an App for password management that works with Apple and Windows take a look at 'BitWarden'. You can change the settings on your 'Windows' version of Chrome.

Can I get Ransomeware on my iPad

Probably not but if you follow the guidelines above you will probably be safe

Can I be Pwned on an iPad

Yes. Hackers steal your personal data from someone else's system and pretend that they have hacked your computer, providing password knowledge that you think came from your computer

If you receive a threat like this, don't pay, just ignore it. Change your most important passwords

Passwords

By about now you may have realized that scams are often about getting information from you, ideally login credentials. If you use the same credentials repeatedly and they are stolen or you inadvertently give the information as part of a scam the potential losses increase significantly.

You should use unique passwords for every online account.
Where money is involved use two-factor authentication

This is a big topic in its own right and we will have a separate session on it.

What Else Can You Do?

What if you lost your iPad or it was stolen?
Does it require a Pincode to open it, or a fingerprint or facial recognition
It should

If your pin is easy to guess how easy would it be for the 'finder' to get at passwords and personal data. Ask yourself this question and make a change, if needed, following some of the advice above.

Turn on 'FIND MY iPad
Don't Jailbreak your iPad
Make sure that your Apple ID has a complex password

Computer Club

iPad Security

October 2021

Pay attention to press items referring to hacking of computer systems where you may have an account and act promptly if asked to change – do not click links to get to your sites.

Use complex passwords everywhere