



University of
Nottingham

UK | CHINA | MALAYSIA

**“It works for
someone, but not
for me”**

**The ongoing challenge
of usable security**

Prof. Steven Furnell

School of Computer Science



Introduction

- Technology alone cannot ‘solve’ security
 - the attitudes, awareness, behaviour and capabilities of users can have significant influence
- Factors such as lack of understanding and unreasonable demands from technologies can impact and impede users’ security efforts
- Technology designers/developers/providers have a significant role to play in helping to overcome the challenges



Cyber Security - Some uncomfortable truths

- It requires us to do things that may not come naturally
 - and in some cases, things we actively don't want to do!
- It isn't normally the thing that we have set out to do when using the technology
 - there are normally a variety of 'must do' tasks to be addressed
- When we use it, we often don't enjoy the experience
 - security often gets in the way and can be regarded as a nuisance





Affecting Perceptions



- Often a mismatch between what we *want*, *need* and *get* in relation to security
- Applies to:
 - support from those providing or expecting them to use it (e.g. websites, employers)
 - support from the technologies they are expected to use
- Can affect how we end up perceiving it ...



Possible Perceptions



- Security is our *friend*!
 - A Guardian Angel
 - Blocks threats
 - Safeguards data
 - Provides reassurance
 - Enables activity



Possible Perceptions

- Security is our *enemy*!
 - Gets in the way
 - Makes things take longer
 - Says 'No'!
 - Makes us worry
 - Inhibits activity





It's not just about perception ...

- People are often characterised as “the weakest link” in cyber security
- This is often because they make *mistakes* – and let's remember ... ‘to err is human’
- Cybersecurity-related mistakes can occur for different reasons:
 - fundamental lack of knowledge and understanding
 - poorly presented technologies
 - unclear/ambiguous rules or processes
 - rushed or pressured decisions



Overcoming the weakest link

- Characterising people as the weakest link is often *correct*
 - it is often their action (or lack of it) that leads to a breach
- But is the characterisation *fair* and is it *avoidable*?
 - are people placed in a context where they are lined up to fail?
 - is enough done to support them to know and do better
- Related responsibilities sit with the designers/providers of security controls, as well as with organisations in which the people are working



Usable Cyber Security



Something to keep in mind ...

“The way to make security that works is to make security that works for people”

www.ncsc.gov.uk/speech/people--the-strongest-link



Something we *need* but not something we *want*

- No-one buys a computer in order to use security features
- Security is, at best, a necessary evil
 - and often it's just a nuisance
- Implications:
 - If people think they can manage without security, they will ignore it
 - If security is too difficult to use, people won't use it
 - If it gets in the way, people will switch it off



Not a new issue

Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

J. D. Tygar¹
EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu

Abstract

User errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent. Is this simply due to a failure to apply standard user interface design techniques to security? We argue that, on the contrary, effective security requires a different usability standard, and that it will not be achieved through the user interface design techniques appropriate to other types of consumer software.

To test this hypothesis, we performed a case study of a security program which does have a good user interface by general standards: PGP 5.0. Our case study used a cognitive walkthrough analysis together with a laboratory user test to evaluate whether PGP 5.0 can be successfully used by cryptography novices to achieve effective electronic mail security. The analysis found a number of user interface design flaws that may contribute to security failures, and the user test demonstrated that when our test participants were given 90 minutes in which to sign and encrypt a message using PGP 5.0, the majority of them were unable to do so successfully.

We conclude that PGP 5.0 is not usable enough to provide effective security for most computer users, despite its attractive graphical user interface, supporting our hypothesis that user interface design for effective security remains an open problem. We close with a brief description of our continuing work on the development and application of user interface design principles and techniques for security.

¹ Also at Computer Science Department, Carnegie Mellon University (on leave).

1 Introduction

Security mechanisms are only effective when used correctly. Strong cryptography, provably correct protocols, and bug-free code will not provide security if the people who use the software forget to click on the encrypt button when they need privacy, give up on a communication protocol because they are too confused about which cryptographic keys they need to use, or accidentally configure their access control mechanisms to make their private data world-readable. Problems such as these are already quite serious: at least one researcher [2] has claimed that configuration errors are the probable cause of more than 90% of all computer security failures. Since average citizens are now increasingly encouraged to make use of networked computers for private transactions, the need to make security manageable for even untrained users has become critical [4, 9].

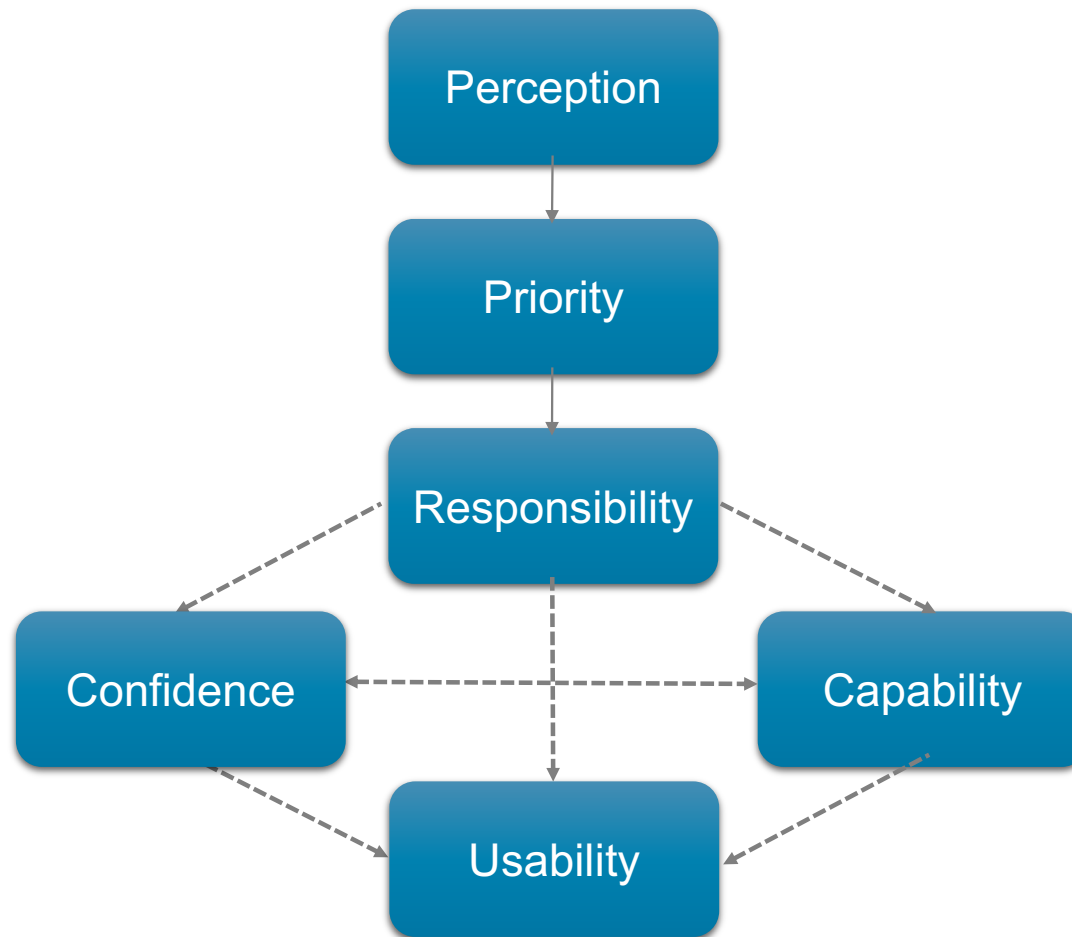
This is inescapably a user interface design problem. Legal remedies, increased automation, and user training provide only limited solutions. Individual users may not have the resources to pursue an attacker legally, and may not even realize that an attack took place. Automation may work for securing a communications channel, but not for setting access control policy when a user wants to share some files and not others. Employees can be required to attend training sessions, but home computer users cannot.

Why, then, is there such a lack of good user interface design for security? Are existing general user interface design principles adequate for security? To answer these questions, we must first understand what kind of usability security requires in order to be

- Seminal paper from 1999
- Not the first mention of usability in a security context, but widely-cited since
- Other works in the same era flagged other problems with usability, from both clarity and performance perspectives



The ultimate security hurdle?



(Furnell, 2010)



What *is* usability?

- ISO 9241–11:2018 defines usability as:

‘The effectiveness, efficiency and satisfaction with which specified users achieve specified goals in particular environments’
- The criteria by which usability is assessed are:
 - *effectiveness*: the accuracy and completeness with which specified users can achieve specified goals in particular environments;
 - *efficiency*: the resources expended in relation to the accuracy and completeness of the goals achieved;
 - *satisfaction*: the comfort and acceptability of the work system to its users and other people affected by its use.



Fitting tasks to the human

In practice, making security usable means establishing a fit with four key elements:

1. the capabilities and limitations of the target users
2. the goals those users have, and the tasks they carry out to achieve them
3. the physical and social context of use
4. the capabilities and limitations of the device on which the security mechanism is used

M. A. Sasse, S. Brostoff, and D. Weirich, “Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security,” *BT Technology Journal*, vol. 19, no. 3, pp. 122–131, 2001.



Give us a CLUE

<u>C</u> onvenient	<ul style="list-style-type: none">▪ Need to maintain balance - security should not be so visible that it becomes intrusive or impedes performance▪ We are likely to disable features that interfere with legitimate use
<u>L</u> ocatable	<ul style="list-style-type: none">▪ We need to be able to find the features we need▪ If we have to spend too long looking, we may give up and remain unprotected
<u>U</u> nderstandable	<ul style="list-style-type: none">▪ We should be able to determine and select the protection we require▪ The technology should not make unrealistic assumptions about our prior knowledge
<u>E</u> vident	<ul style="list-style-type: none">▪ We ought to be able to determine whether protection is being applied and to what level▪ Appropriate status indicators and warnings will help to remind us if safeguards are not enabled



Too much to tolerate?

- Confusing
- Distracting
- Time-consuming
- Inconsistent
- Insufficient



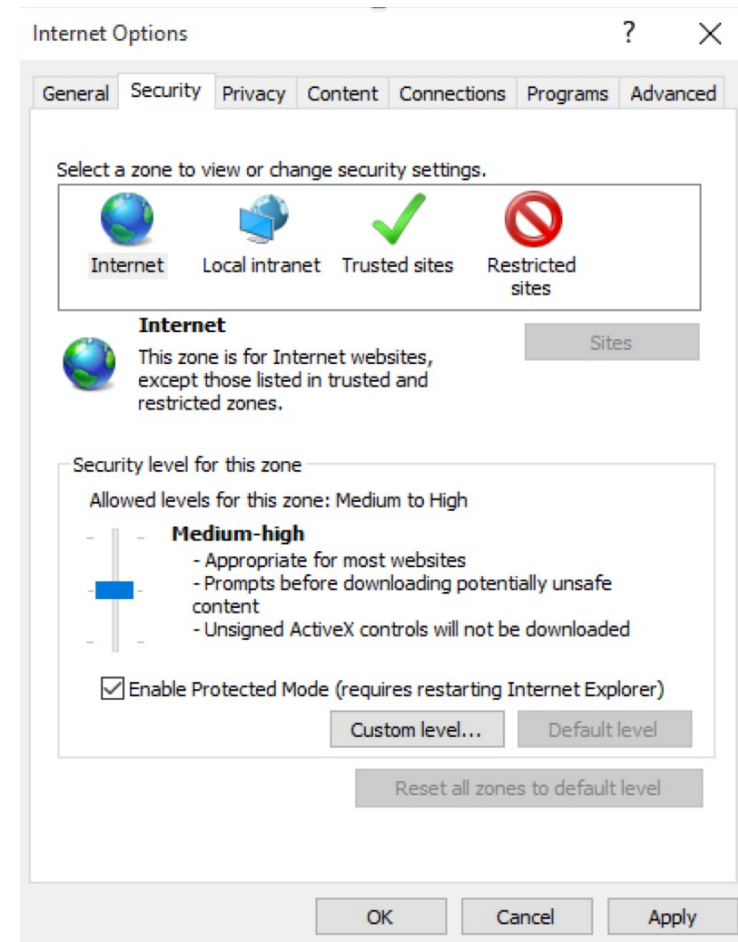


A classic example



My 'go to' example of 'bad'

The Security Settings within *Internet Explorer 11*





Spot the difference ...



Medium

- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded



Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

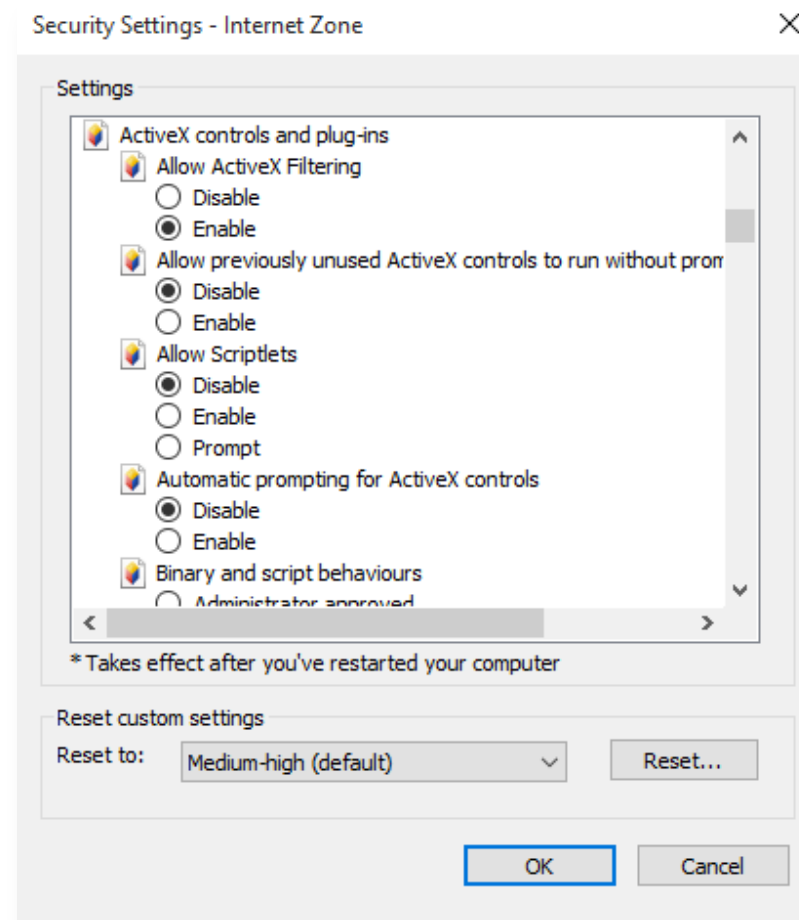


High

- Appropriate for websites that might have harmful content
- Maximum safeguards
- Fewer secure features are disabled



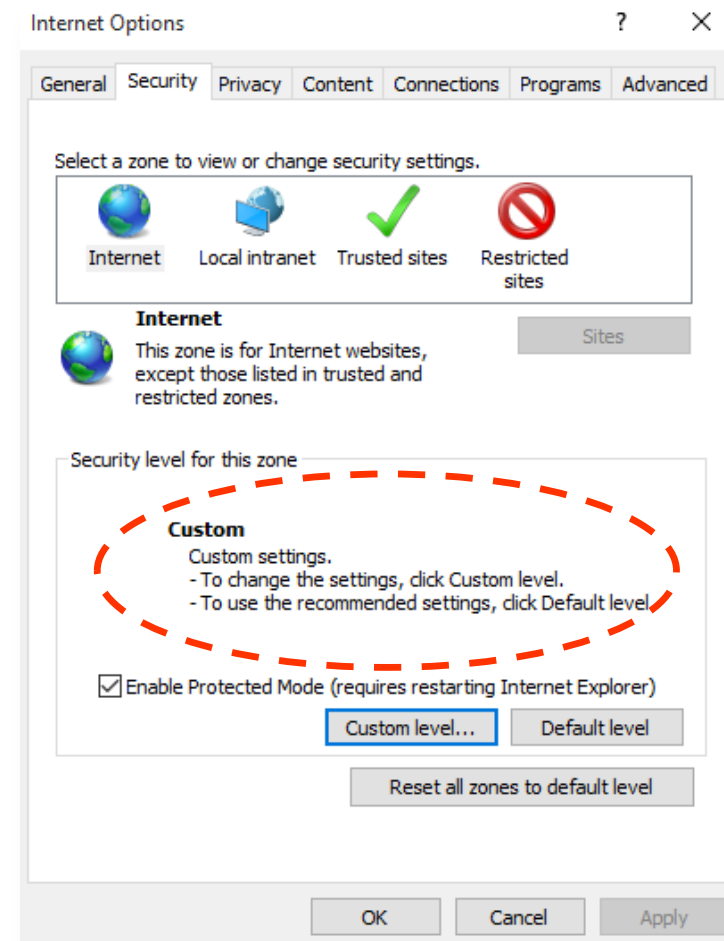
IE 11's Custom Security settings





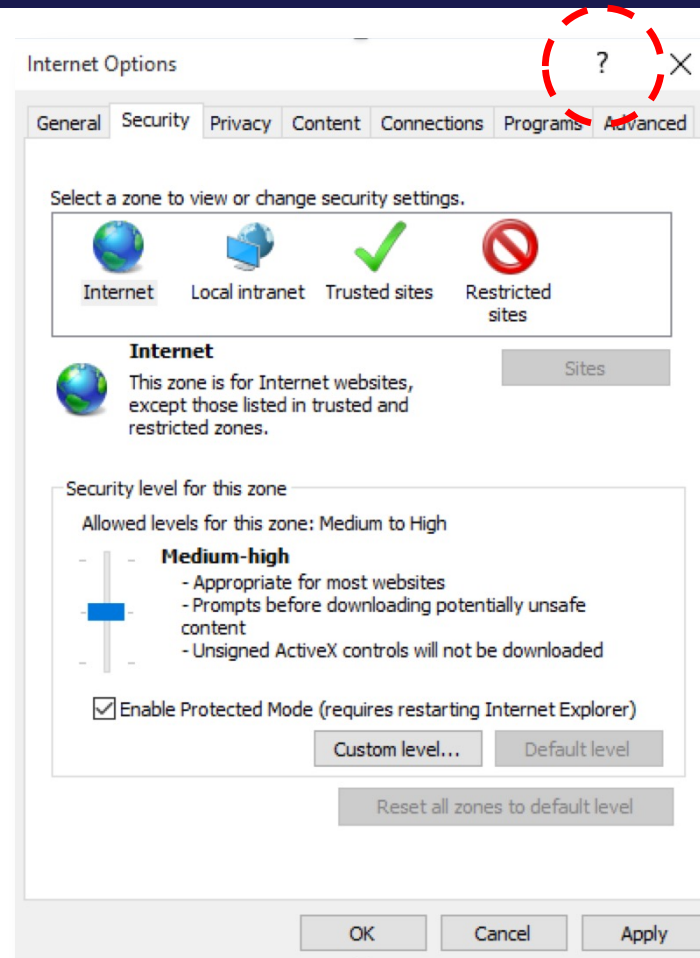
Where has the slider gone?

Having gone into the Custom settings, you no longer get any indication of your level of protection





Hold on, maybe I'm missing something





So, was I missing something?

Change security and privacy settings for Internet Explorer 11

Email

Print

Note

Go to the bottom of the page to get help for older versions of Internet Explorer. [Which version of Internet Explorer am I using?](#)

Privacy settings

By adjusting Internet Explorer's privacy settings, you can affect how websites monitor your online activity. For example, you can decide which cookies are stored, choose how and when sites can use your location info, and block unwanted pop-ups.

Show All

- ▼ Cookies
- ▼ Do Not Track
- ▼ InPrivate Browsing
- ▼ Location
- ▼ Pop-up Blocker
- ▼ Tracking Protection

Security zones

By changing the security settings, you can customize how Internet Explorer helps protect your PC from potentially harmful or malicious web content. Internet Explorer automatically assigns all

Not much of obvious
use here

Let's look at Security
Zones ...



Help?

Security zones

By changing the security settings, you can customize how Internet Explorer helps protect your PC from potentially harmful or malicious web content. Internet Explorer automatically assigns all websites to a security zone: Internet, Local intranet, Trusted sites, or Restricted sites. Each zone has a different default security level that determines what kind of content might be blocked for that site. Depending on the security level of a site, some content might be blocked until you choose to allow it, ActiveX controls might not run automatically, or you might see warning prompts on certain sites. You can customize the settings for each zone to decide how much protection you do or don't want.

[Show All](#)


- ▼ [Change your security zone settings](#)
- ▼ [Add or remove a site from a security zone](#)
- ▼ [Turn on Enhanced Protected Mode](#)

Nothing yet
to explain
what the
actual
Settings
mean



Help!

^ Change your security zone settings


1. Open Internet Explorer, select the **Tools** button , and then select **Internet options**.
2. Select the **Security** tab and customize your security zone settings in these ways:
 - To change settings for any security zone, select the zone icon, and then move the slider to the security level that you want.
 - To create your own security settings for a zone, select the zone icon, and then select **Custom level** and choose the settings that you want.
 - To restore all security levels to their original settings, select the **Reset all zones to default level** button.

**Still nothing
to explain
what the
Settings
mean**



Help!!

^ Add or remove a site from a security zone

1. Open Internet Explorer, select the **Tools** button , and then select **Internet options**.
2. Select the **Security** tab, choose one of the security zone icons (**Local intranet**, **Trusted sites**, or **Restricted sites**), and then select **Sites**. You can add sites to the zone you chose, or delete sites that you no longer want in this zone.
3. If you chose **Local intranet** in the previous step, select **Advanced**, and then do one of the following:
 - **Add a site.** Enter a URL into the **Add this website to the zone** box, and then select **Add**.
 - **Remove a site.** Under **Websites**, select the URL you want to remove, and then select **Remove**.

Still nothing
to explain
what the
Settings
mean

(Spotting a
pattern yet?)



Help!!!

^ Turn on Enhanced Protected Mode

Enhanced Protected Mode makes it harder for malware to run in Internet Explorer.

To turn on or off Enhanced Protected Mode

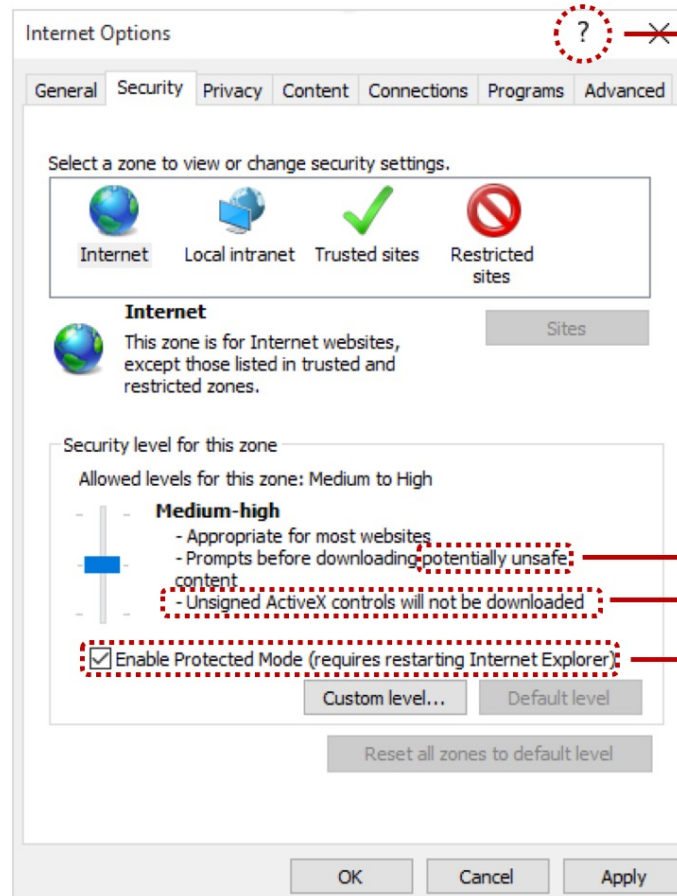
1. Open Internet Explorer, select the **Tools** button, and then select **Internet Options**.
2. On the **Advanced** tab, under **Security**, select (or clear) the **Enable Enhanced Protected Mode** check box, and then select **OK**. You'll need to restart your PC before this setting takes effect.

Of course, still nothing to explain the Settings

Meanwhile, what *is* Enhanced Protected Mode?
We *know* how to turn it on – we were already on that screen!
What does it *do*, and why would I *not* want to use it?



So, in summary ...



Although context-sensitive Help is *available*, none of the questions below are answered

What content would this be in practice?

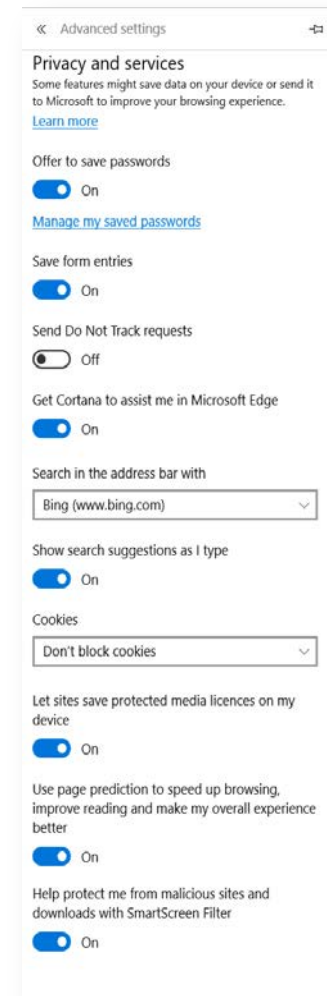
What are Unsigned ActiveX controls?

What is Protected Mode?



Getting an Edge?

- Ground-up redesign of the browser
 - engineered-out various aspects that would have required users to have an additional security interactions and decisions
 - heralded as a more secure application
- Leaves users free to focus upon aspects that they can relate to and see as relevant
 - no longer concerned with security zones and levels
 - just ten settings - less to understand and less to potentially misconfigure





More recent examples



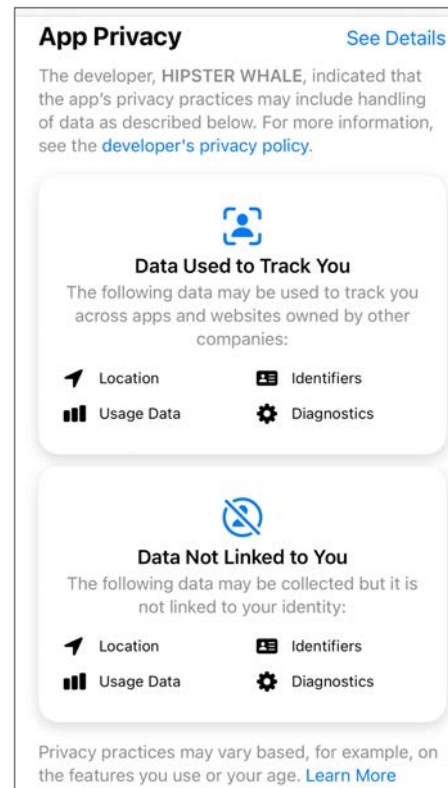
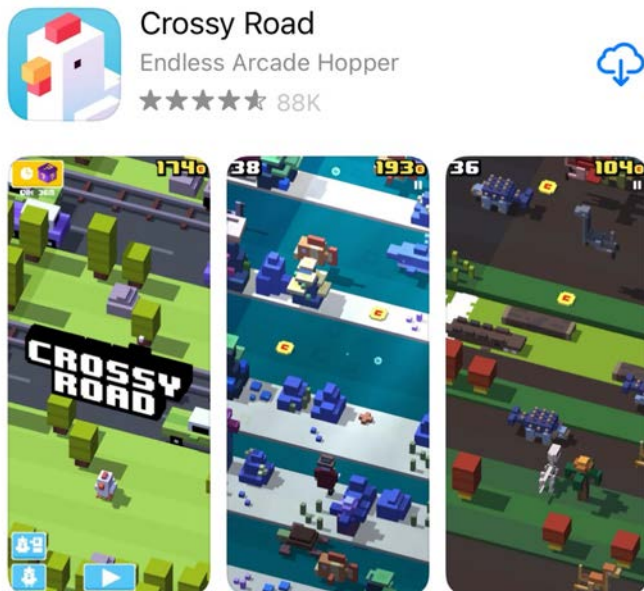
App permissions and privacy

- A context in which the user may 'see' what access an app will obtain to their device and data
- Not necessarily an option to *control* it
- App Stores provides the basis for a decision before downloading the app
- But is it an *informed* decision?

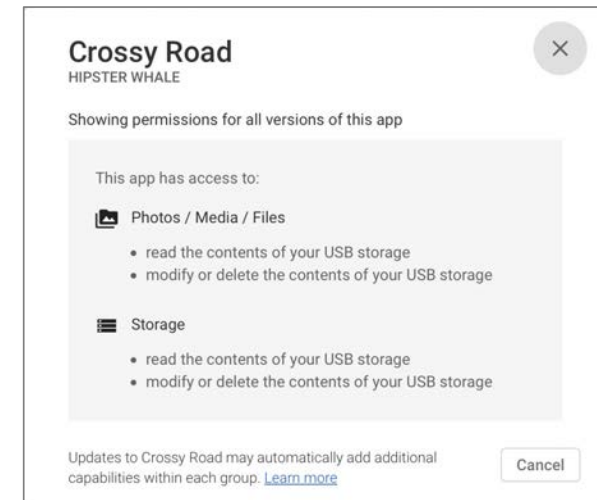




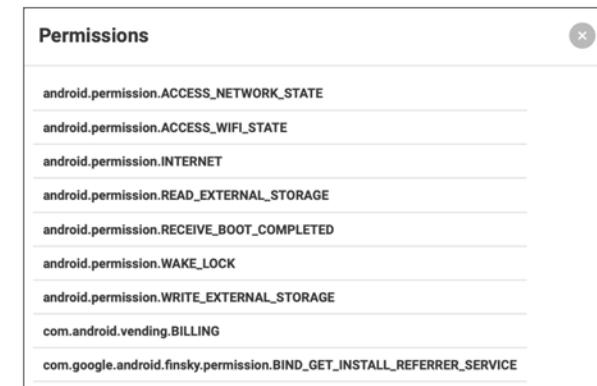
Permissions ... same app, different stores



App Store



Google Play



Aptoide



What do the permissions *mean*?

App Privacy [See Details](#)

The developer, HIPSTER WHALE, indicated that the app's privacy practices may include handling of data as described below. For more information, see the [developer's privacy policy](#).

Data Used to Track You

The following data may be used to track you across apps and websites owned by other companies:

- Location
- Identifiers
- Usage Data
- Diagnostics

Data Not Linked to You

The following data may be collected but it is not linked to your identity:

- Location
- Identifiers
- Usage Data
- Diagnostics

Privacy practices may vary based, for example, on the features you use or your age. [Learn More](#)

Data Used to Track You

The following data may be used to track you across apps and websites owned by other companies:

- Location
 - Coarse Location
- Identifiers
 - User ID
 - Device ID
- Usage Data
 - Product Interaction
 - Advertising Data
 - Other Usage Data
- Diagnostics
 - Crash Data
 - Performance Data
 - Other Diagnostic Data

Items listed under each heading reflect what this specific app is collecting

Usage data

Product interaction

Such as app launches, taps, clicks, scrolling information, music-listening data, video views, saved place in a game, video or song, or other information about how you interact with the app.

Advertising data

Such as information about the advertisements you have viewed.

Other usage data

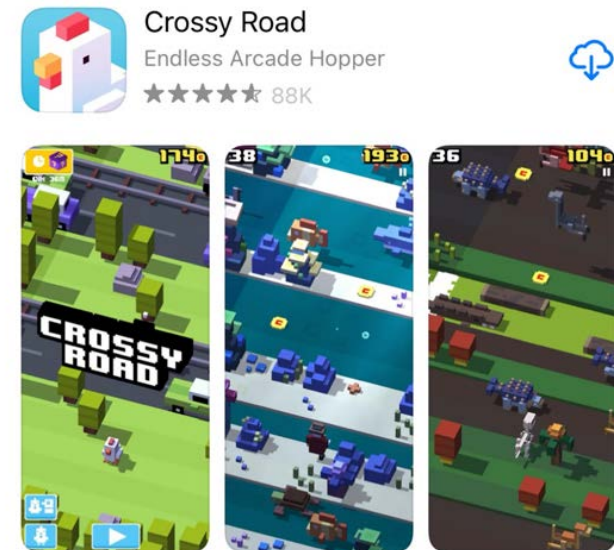
Any other data about your activity in the app.

The descriptions here are Apple's generic indicators of what the permissions mean



Unanswered questions

- Why does Crossy Road *need* these permissions?
- What is the app or the developer going to *do* with the data it collects?
- And all the while, the user is told about the permissions butx has no *control* over them





Cookies – another example of ‘same but different’

(a)

We value your privacy

We and our partners store or access information on devices, such as cookies and process personal data, such as unique identifiers and standard information sent by a device for the purposes described below. You may click to consent to our and our partners' processing for such purposes. Alternatively, you may click to refuse to consent, or access more detailed information and change your preferences before consenting. Your preferences will apply to a group of websites. Please note that some processing of your personal data may not require your consent, but you have a right to object to such processing. You can change your preferences at any time by returning to this site or visit our privacy policy.

REJECT ALL **ACCEPT ALL**

Store and/or access information on a device	OFF >
Select basic ads	OFF >
Create a personalised ads profile	OFF >

PARTNERS **LEGITIMATE INTEREST** **SAVE & EXIT**

(b)

Manage cookies

Choose the cookies that work for you. If you need more information, please see our cookies notice.

Essential **Always Active**

Some cookies are essential – our website wouldn't work without them! We collect them to keep our website secure and ensure that from browsing to booking, your online experience runs smoothly.

Performance (Recommended)

These cookies help us understand user experiences. We'll never use them to identify you personally – just to monitor how well our website is working and if there's any room for improvement.

Experience

We use these cookies to personalise your experience – tailoring content throughout your visit. We also use these cookies to test new website features and improve functionality across our website.

Marketing

These cookies allow us to tailor the advertising you receive from [redacted]. Without these cookies you would still receive adverts – they would just be less relevant to you.

Confirm settings

COOKIE PREFERENCES **Close X**

Cookies we use on this site

Necessary ☒

Necessary cookies help make a website usable by enabling basic functions like page navigation and access to secure areas of the website. The website cannot function properly without these cookies.

Marketing ☐

Marketing cookies are used to track visitors across websites. The intention is to display ads that are relevant and engaging for the individual user and thereby more valuable for publishers and third party advertisers.

Statistics ☐

Statistic cookies help website owners to understand how visitors interact with websites by collecting and reporting information anonymously.

Allow selection

Allow all

(c)

We use cookies

Our website uses essential cookies to function properly. These cookies cannot be switched off and do not store any of your information. We also use the non-essential cookies listed below but only if you agree. Please use the buttons below to let us know your preferences. We use "analytical" cookies to better understand and improve the way our website works. Read more about the individual cookies we use and how to control the use of cookies in our [Cookie Policy](#).

Learn more **Reject** **Accept**

(d)



Variations by default

- (a) and (c) enable the user to Reject all optional cookies with one click, but others do not
- (b) and (d) provide brief explanations of their settings, (a) does not
- (a) and (d) set all optional settings 'off' by default, whereas (b) defaults all to 'on' and has the 'Confirm settings' highlighted, increasing the chance to accept everything (potentially in error)
- (c) conceals details individual cookie settings unless you 'Learn more'. If you 'Accept' from the initial dialogue, you have no clear indication of *what* settings are accepted
- (d) shows the 'Necessary' cookies as a pre-selected checkbox that the user cannot change
- (d) has 'Allow all' to select everything, but no corresponding 'Reject all'



Smart TVs ... the variation continues



LG 55UH7700
(2016)



Samsung UE50KU6000K
(2016)



Sony Bravia XR XR55A80J
(2021)

- All download and install apps, browse the web, store media (music/photos/videos), connect to external devices
- All have options for Software Update to keep apps and system software up-to-date, but beyond this ...



Security options and usability



LG 55UH7700
(2016)

- Appears to have nothing related to security
 - the closest is a 'Safety' menu to set a PIN to control access to applications, inputs (sources), and programmes (channels)
- User conclusion:
 - Security is not an issue, as there are no settings to worry about



Security options and usability



Samsung UE50KU6000K
(2016)

- Has ‘Smart Security’ options buried away within an ‘Expert Settings’ section of the overall ‘System’ settings.
 - these “protect your TV from hackers, spyware, and viruses
 - include the options to scan the device for malware, and to enable/disable Real-Time Monitoring
- A PIN-based lock to prevent changes to channels/tuning, as well as restrict access to the apps (but the latter is not done via the main device settings)



Security options and usability



Samsung UE50KU6000K
(2016)

- User conclusions:
 - there are some settings related to malware protection – there is presumably a risk from this
 - there is an option to monitor for it in real time, and so if that is on, we can assume we are as protected as possible



Security options and usability



Sony Bravia XR XR55A80J
(2021)

- Supports user accounts and sign-in (with sub-options for payment authentication and permitting the use of the voice assistant)
- Parental controls (which links to the PIN-based restrictions for channels, inputs and apps)
- An Apps menu (including sub-options for 'App permissions' and Security 'restrictions')
- A distinct Privacy menu with sections for devices, account and app-related settings (including some of the options also accessible via other menu routes)



Security options and usability



Sony Bravia XR XR55A80J
(2021)

- User conclusions:
 - Dealing with security and privacy appears to be a something of a challenge, as there is quite a confusing array of settings
 - It takes a while to navigate around to:
 - find them all
 - get a sense of whether everything is setup as desired



Reflections

- What we see across these ‘broader context’ examples is that:
 - all bring security and privacy issues with them
 - the default in each case still has significant potential to leave users feeling that things fall of following ISO usability principles
- For example, we see approaches that users may feel are:
 - not *effective* (e.g. the lack of real insight or control with the privacy labels)
 - not *efficient* (e.g. the varying demands of the cookie settings)
 - not *satisfying* (e.g. the varying presence or absence of features across different smart devices)
- There is perhaps some way to go before usable security can be relied upon



“Have you looked at the privacy and permissions settings?”



“I would have assumed that they had them, but I've never really given it that much thought. I've never looked at the privacy settings. No.”

“I feel like I probably know that they have those settings, but I don't think I've ever looked them in great detail.”

“I trust that the speaker has kind of built in settings. I don't necessarily look at them personally.”

“Yes, I know about them. And no, I haven't looked at them.”

“I haven't because I didn't know how to do it or I didn't know I needed to do it, and I didn't know it existed.”

“I'm aware of it. I've never looked into it.”

(Heer, Alghamdi and Furnell, 2023)



Conclusions



Conclusions

- It is too easy to focus upon technology and forget the people that use it
- Security is meant to support and protect us
 - it should not become the source of frustration!
- Security does not *have* to be difficult to use
 - poor design and lack of consideration often ensures that it is
- Making security-related options *available* is not enough
 - need to consider usability, clarity, overheads
 - if we cannot use the features, we remain unprotected
- Need to ensure that the technology does not stand in the way
 - unusable security may be as good as none at all



A few questions to consider

- Clarity
 - Can the user understand it?
 - Can they get help?
- Overhead
 - Is it requiring too much time?
 - Is it interrupting something?
 - Does it affect other programs?
 - Does the user *have* to see it?
- Configurability
 - Does it allow users to do what they are likely to want/expect?





**University of
Nottingham**

UK | CHINA | MALAYSIA

Prof. Steven Furnell

steven.furnell@nottingham.ac.uk

[@smfurnell](#)