# Sun City Computer Club

Safer WEB Browsing

Safer WEB Browsing Class video

**Audio Recording & video at link**

# Advantages to PowerPoint delivery

- Any length
- Any time
- Any schedule
- Timeliness
- Pause and continue
- Pause and look up for clarity
- Skip over
- Play again and again
- Adjust video size
- Adjust audio level
- Available to new users  Months from now

- No Questions
- No visual feedback

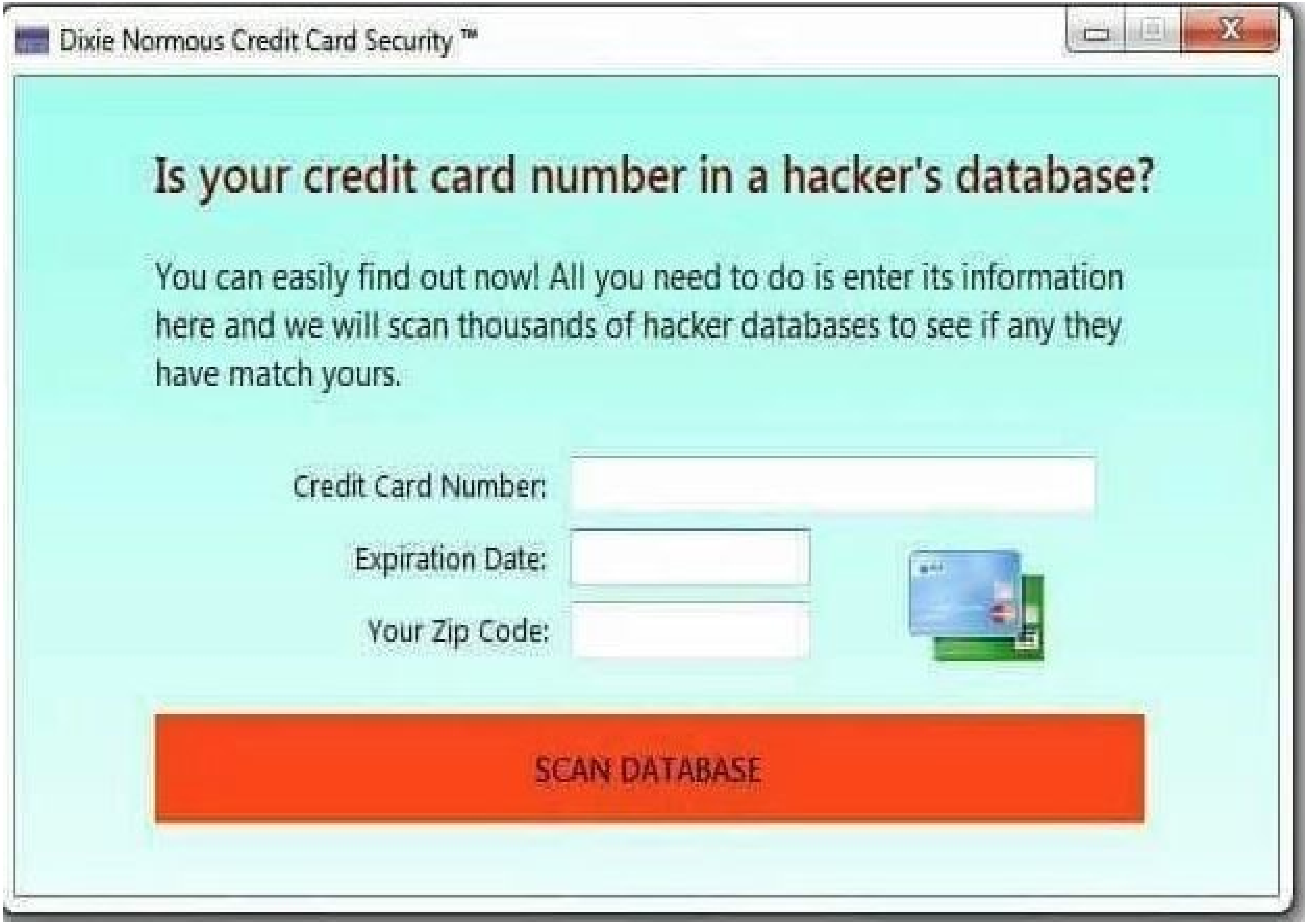
# Disadvantages of PowerPoint Delivery

# Vocabulary

- Safer not Safe
- E-postcard not e-mail
- ADMINISTRATOR

Sun City Computer Club Cyber Security News BLOG - Administrator

- Passphrases not passwords
  Credential spraying
- Radio not wireless
- Identity cloning
- Helpful <-> Harmful



Dixie Normous Credit Card Security ™

# Is your credit card number in a hacker's database?

You can easily find out now! All you need to do is enter its information here and we will scan thousands of hacker databases to see if any they have match yours.

| | |
|---|---|
| Credit Card Number: | |
| Expiration Date: | |
| Your Zip Code: | |

- First job computing 1962
- 9 years semi-conductor manufacturer
- 30 years Cyber engineer Major Oil Co.
- Very early WEB experience
- 3 years Alyeska Pipeline
- Major Cyber Security Certifications
- Network of cyber professionals
- Computer Club presentations
- Cyber Security SIG, Windows SIG
- Senior University Cyber topics

# What does John know

- Trust
- Convenience

- FOMO
- Curiosity

- Any/everyone can have a voice

# Fundamental Issues

- Over a BILLION web sites
- Over 4 billion users on Internet
- If you can see them, they can see you

- Connectionless
- Not intended for current use
- Query & Response
- Client Server

  either can run code on the other
- Any/everything apps, attachments, audio, video
- Interpreters/helpers
- ActiveX, Java, scripts, shells
- HTTP
- HTML

# WEB issues

- Akamai, cloud
- Increased use of third party services
- What, me worry?
- Information gives no indication of being stolen
- Information is cumulative

# WEB issues

# Journey to the Web site

- Name resolution

  Own name, Hosts file, NetBIOS, DNS

- Domain Name System

  Distributed, hierarchical, caching database

  No authentication

- BGP

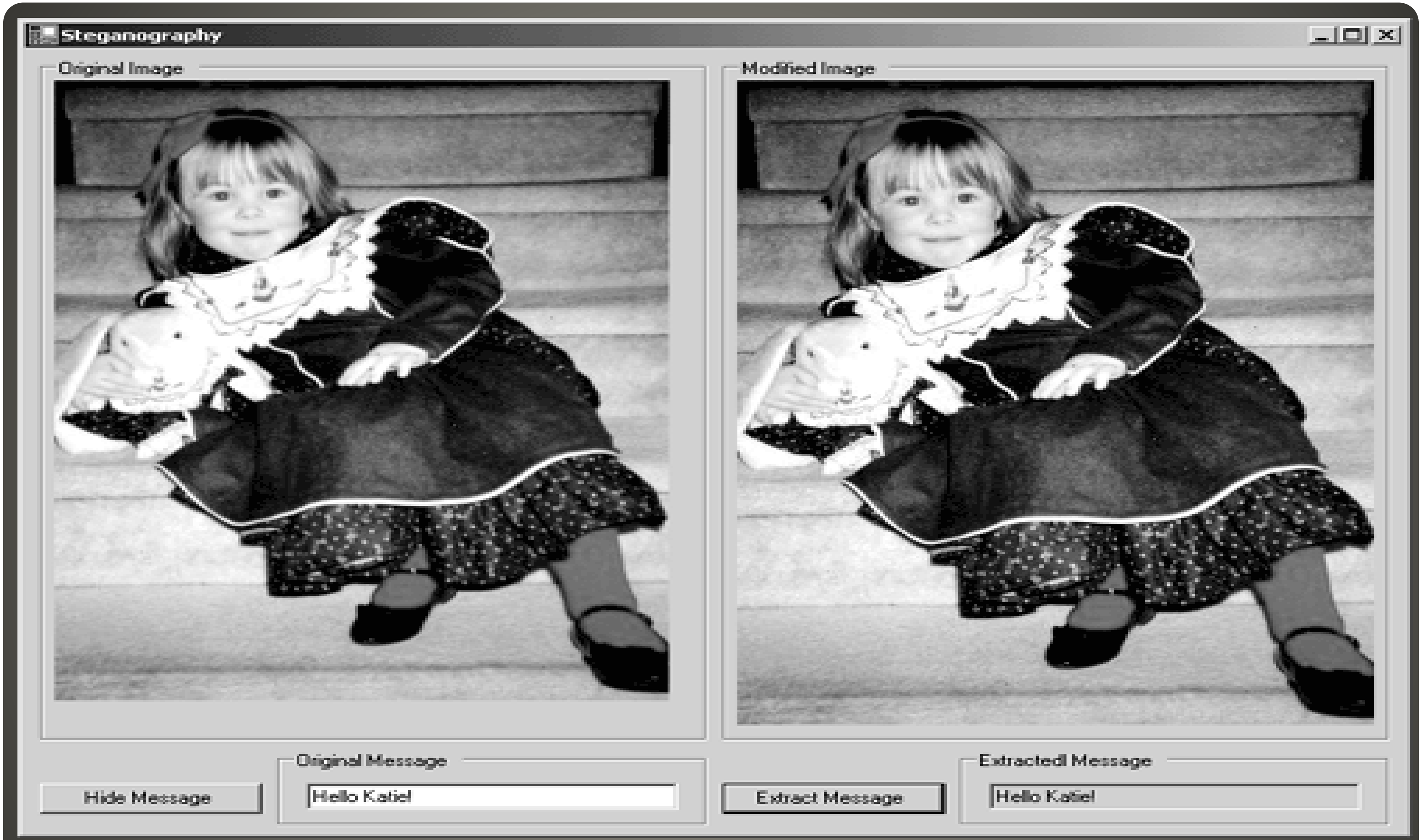
  routing, No authentication

# cryptography

- 1-2-3-4
- Steganography
- Hash
- Symmetric
- Asymmetric

# cryptography

- 1-2-3-4
- Algorithm
- Key
- Plain text
- Cypher text



Original Message: Hello Katie!

Extracted Message: Hello Katie!

# Steganography

# hash

- One way
- Fixed length output
- Any length input
- Message digests
- E.g. MD2,MD4,MD5,SHA-1,SHA-2
- Used for integrity, digital signing & passphrases

# symmetric

- Plain text, algorithm, key, cypher text
- Algorithm usually public
- Key space is important
- Reversible with the one key
- Does not scale
- E.g. RC4,SEAL  DES,3DES,RC5,Rijndael
- One-time pad
- Cryptanalysis
- Control

# CIA

- Confidentiality
- Integrity
- Authentication
- Non-Repudiation

- Public & private key
- Intractable problem
- Symmetric key exchange in presence of advisory
- Thousands of times slower
- E.g. RSA, El Gamal, ECC
- Public key distributed and verified via Digital Certificate
- Signing via digital signature

# Asymmetric

# Uses of cryptography

- Code signing
- VPN
- Confidentiality
- Integrity
- Authentication
- Non-Repudiation
- Disk and file encryption
- IPSec
- PKI
- blockchain

- Client hello
- Server hello
- Client validation and pre-master secret
- Both sides use secret to generate session key(s)
- Web session proceeds with data in transit encrypted with symmetric key(s)

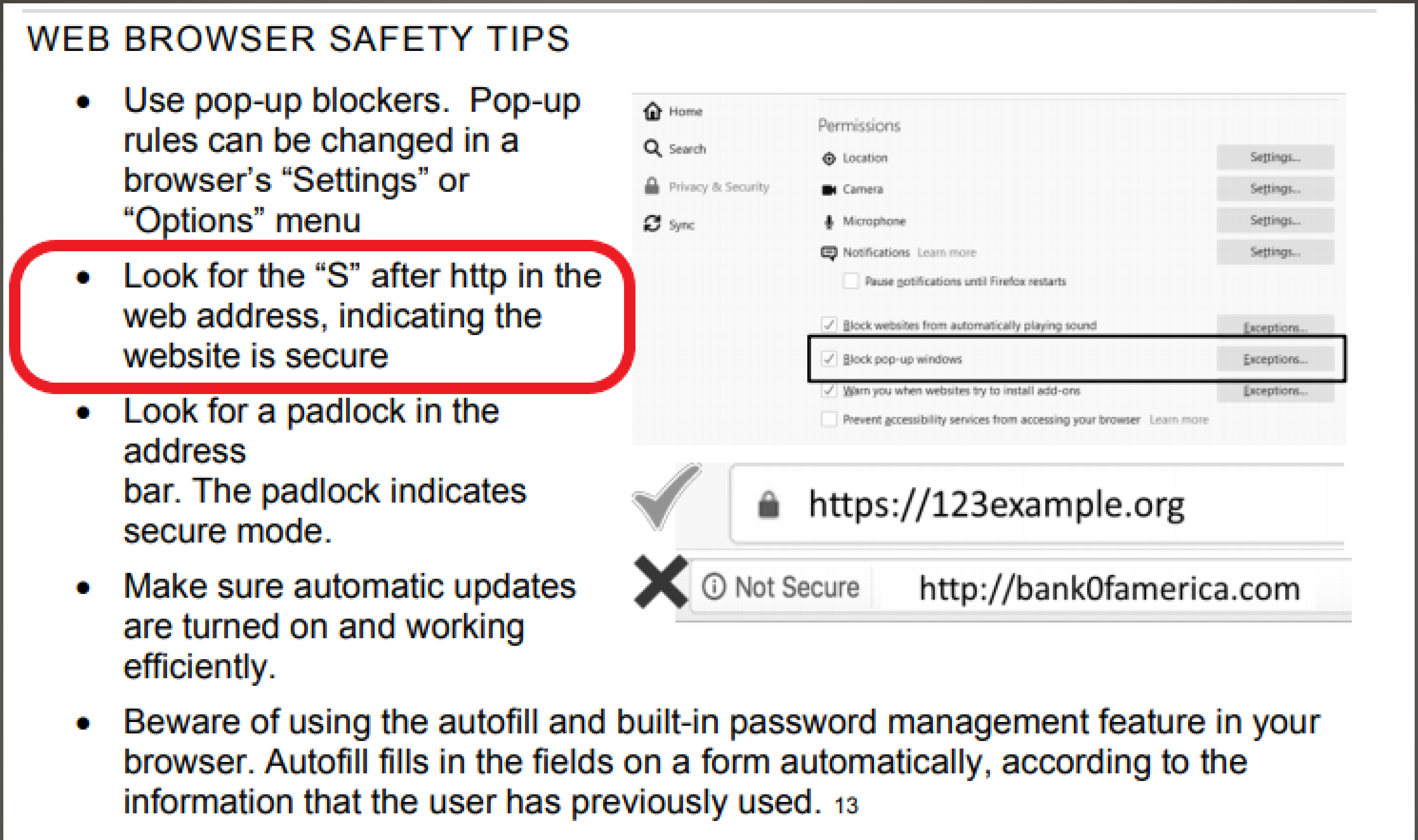
# Some detail

# Digital Certificates

- Part of PKI
- Binding of public key to entity
- Verified and signed by certificate authority
- Chain of trust
- X.509

- SSL TLS
- Asymmetric used to exchange symmetric key

# WEB transit security



## WEB BROWSER SAFETY TIPS

- Use pop-up blockers. Pop-up rules can be changed in a browser's "Settings" or "Options" menu
- Look for the "S" after http in the web address, indicating the website is secure
- Look for a padlock in the address bar. The padlock indicates secure mode.
- Make sure automatic updates are turned on and working efficiently.
- Beware of using the autofill and built-in password management feature in your browser. Autofill fills in the fields on a form automatically, according to the information that the user has previously used. 13

Permissions

Location Settings...
Camera Settings...
Microphone Settings...
Notifications Learn more Settings...
□ Pause notifications until Firefox restarts
☑ Block websites from automatically playing sound Exceptions...
☑ Block pop-up windows Exceptions...
☑ Warn you when websites try to install add-ons Exceptions...
□ Prevent accessibility services from accessing your browser Learn more

✓ https://123example.org

✗ ⓘ Not Secure http://bank0famerica.com

**Semantics Government Safe**

- Virtual machines   Linux
- Live CD/DVD
- Check for updates before each sensitive session
- New browser for each sensitive session
- Clickjacking
- Cross Site Scripting
- Cross Site Request Forgery
- “Private” sessions

# Safer Browsing

- Browser wars
- Brave, Lynx
- Add-ons and extensions

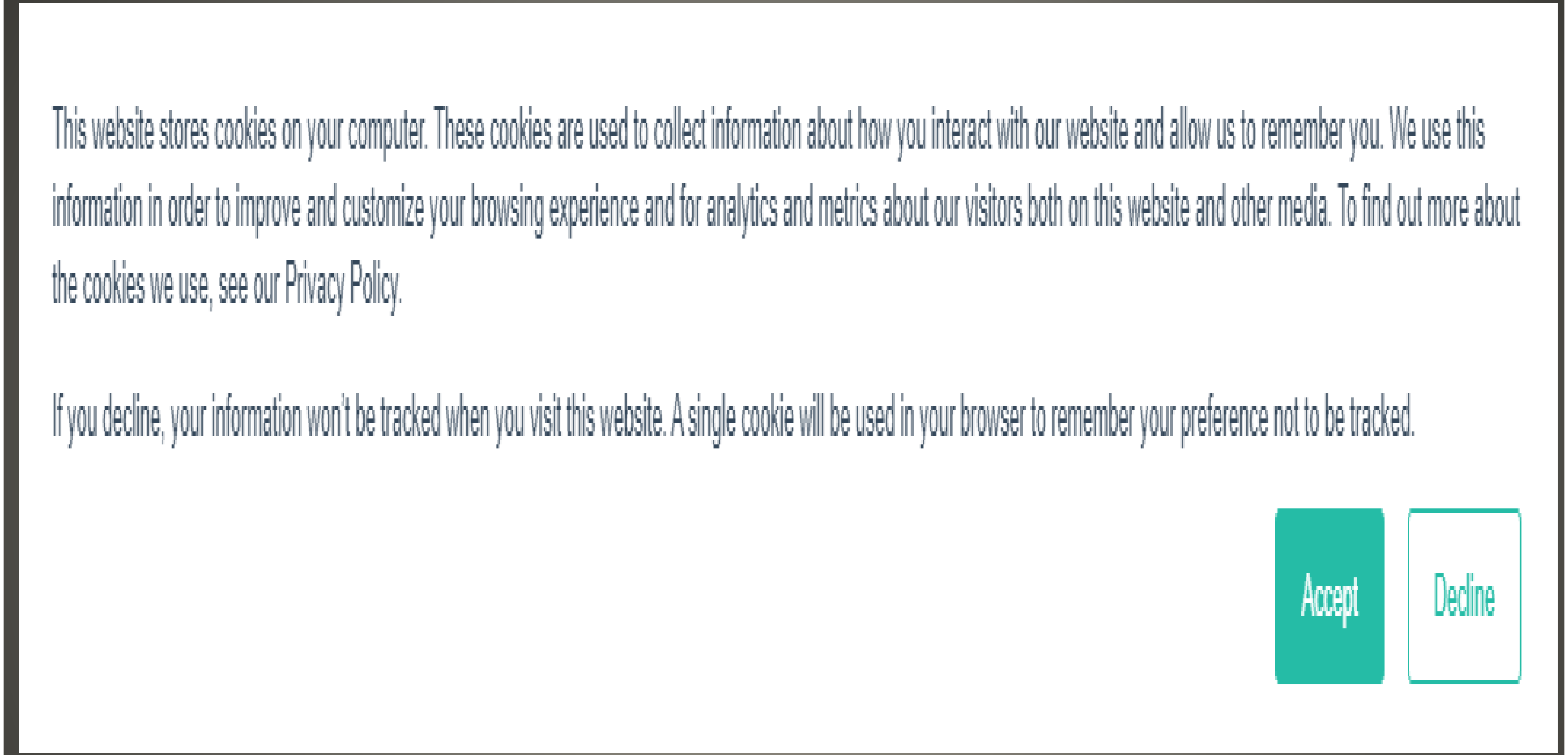
  uBlock Origin, NoScript, uMatrix, AdBlocker
- MultiFactor Authentication
- Maintain state

  URL, Hidden form fields, cookies
- Proxy
- TOR
- Business Practices IRS – Phone Bank - PIN

# Safer Browsing

- Methods
  POST, GET, PUT, PATCH, DELETE
- Response
  1xx Informational
  2xx success
  3xx redirection
  4xx client error
  5xx server error
- Referrer
- Redirect
- F12
- Cookies
  tracking, 3rd party, super, flash,   HTML5, etc.

# HTML



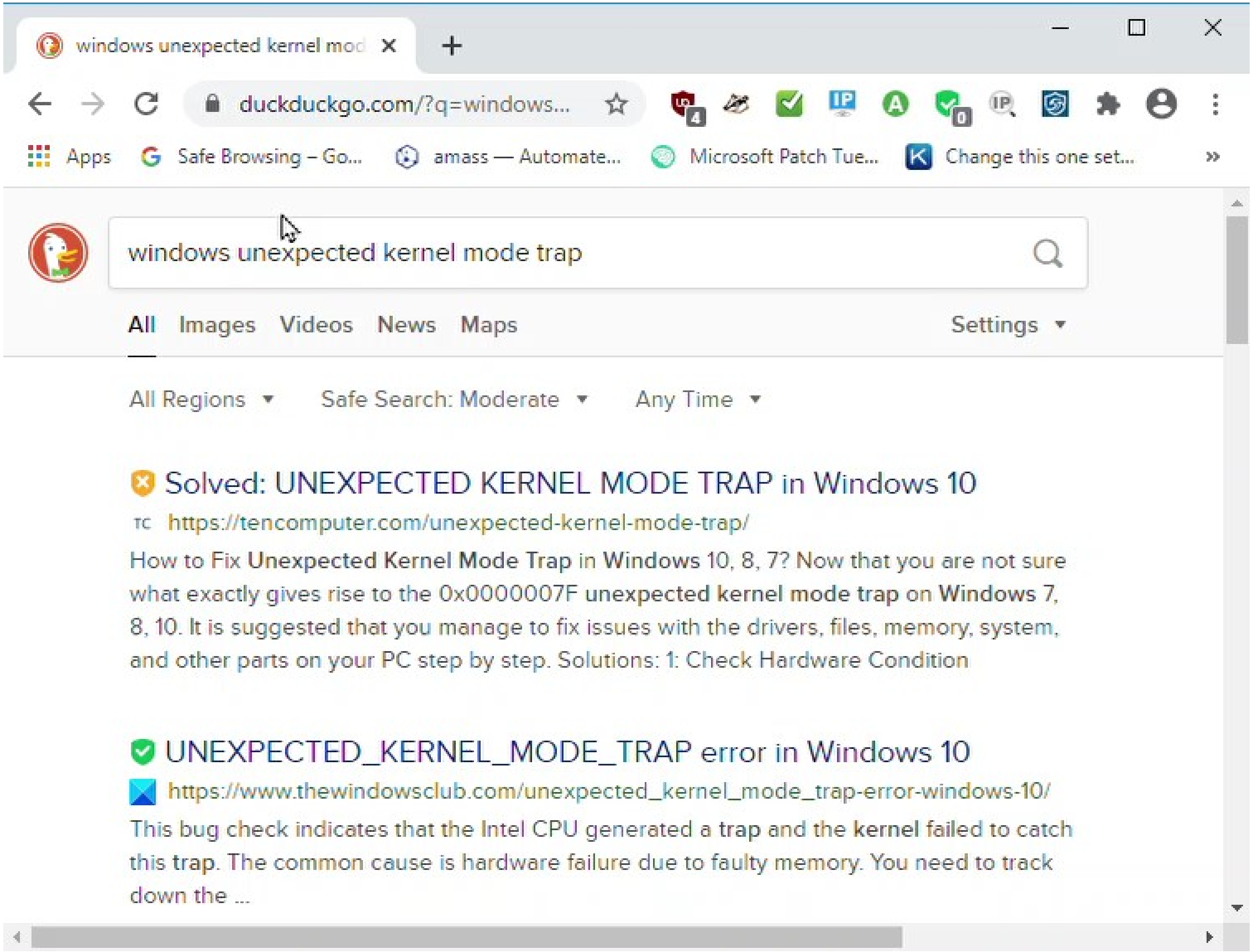
This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy.

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

# Cookies

# Tracking

- Cookies
- IP Address
- History
- Local logs
- Browser User Agent string
- Fingerprinting
- Referrer
- “I am not a robot”
- Anything coders can think of …



windows unexpected kernel mode trap

Solved: UNEXPECTED KERNEL MODE TRAP in Windows 10

https://tencomputer.com/unexpected-kernel-mode-trap/

How to Fix **Unexpected Kernel Mode Trap** in **Windows** 10, 8, 7? Now that you are not sure what exactly gives rise to the 0x0000007F **unexpected kernel mode trap** on **Windows** 7, 8, 10. It is suggested that you manage to fix issues with the drivers, files, memory, system, and other parts on your PC step by step. Solutions: 1: Check Hardware Condition

UNEXPECTED_KERNEL_MODE_TRAP error in Windows 10

https://www.thewindowsclub.com/unexpected_kernel_mode_trap-error-windows-10/

This bug check indicates that the Intel CPU generated a **trap** and the **kernel** failed to catch this **trap**. The common cause is hardware failure due to faulty memory. You need to track down the ...

# Maintaining State

- URL

https://mg.mail.yahoo.com/neo/b/launch?&filterBy=&fid=Inbox&fidx=1&ac=gfVcFbP06soZ0XxbtXJq5aW8I1M-&mailboxId=VjJ-C_UFXi_-EVMadxLtWRtp9zjHo-i8cY1FYym0mI8b9spZcwe1Zg2b-H0cYx2fOJ3OGH4nkLovJSeSm65J6U1w&.rand=1655841https://mg.mail.yahoo.com/neo/b/launch?&filterBy=&fid=Inbox&fidx=1&ac=gfVcFbP06soZ0XxbtXJq5aW8I1M-&mailboxId=VjJ-C_UFXi_-EVMadxLtWRtp9zjHo-i8cY1FYym0mI8b9spZcwe1Zg2b-H0cYx2fOJ3OGH4nkLovJSeSm65J69qU1w&.rand=165584188&nsc88&nsc

- Hidden Form Fields

```
<form action="myform.cgi">
<input type="file" name="fileupload" value="fileupload" id="fileupload">
<label for="fileupload"> Select a file to upload</label>
<input type="hidden" id="ipaddr" name="ipaddr" value="<?php echo $_SERVER['REMOTE_ADDR']; ?>">
<input type="hidden" id="referer" name="referer" value="<?php echo $_SERVER['HTTP_REFERER']; ?>">
<input type="submit" value="submit">
</form>
```

- Cookies

- VMs
- Live CD/DVD/USB
- Search Engine
- Hover Over
- Multiple Browsers
- Multiple security configurations
- VPN
- Tiny URL expansion
- Popups

# Safer

- Certificate warnings
- Drive By
- Sites with user supplied WEB content
- EULA
- Deliberate mistakes
- Become informed, aware, suspicious

# Safer

- URL inspection
- Professionalism
- Surveys & Account creation
- Google Transparency Report
- Lynx
- F12
- BBB
- Intent & AutoFill
- Security Images
- Multi Factor Authentication

# Safer

- Update Update Update Update
- 3-2-1 Backup
- Security Suites   Defense in Depth
- MultiFactor authentication
- https
- VPN
- Deliberate mistakes on Data Entry
- Awareness

# Safer

- DuckDuckGo
- WolframAlpha
- Startpage
- Privatelee
- Yippy
- Hulbee
- Gibiru
- Disconnect Search
- Lukol
- MetaGer

# Search Engines without tracking

- Questions, suggestions, comments?

**SCCCCyber@gmail.com**

- https://heimdalsecurity.com/blog/ultimate-guide-secure-online-browsing/
- https://www.google.com/transparencyreport/
- https://myaccount.google.com/activitycontrols

# Useful Links