

LIVE



breakyourownnews.com

BREAKING NEWS

HOW TO FORGE FAKE NEWS AND...

12:54

SPAWN FLAWLESS PHISHERIES

LIVE

Speaker bio (Who am I?)

Michael Allen ([@Wh1t3Rh1n0](#))

- Pentesting and red teaming for 9+ years
- Red team lead at BHIS
 - Special interest in Initial Access
- Creator and instructor of “[Red Team Initial Access](#)”
 - Exactly how we *currently* break into well-defended, enterprise environments over the internet
 - Available on AntiSyphonTraining.com
- Today’s topic comes straight out of the class. 😊



Agenda

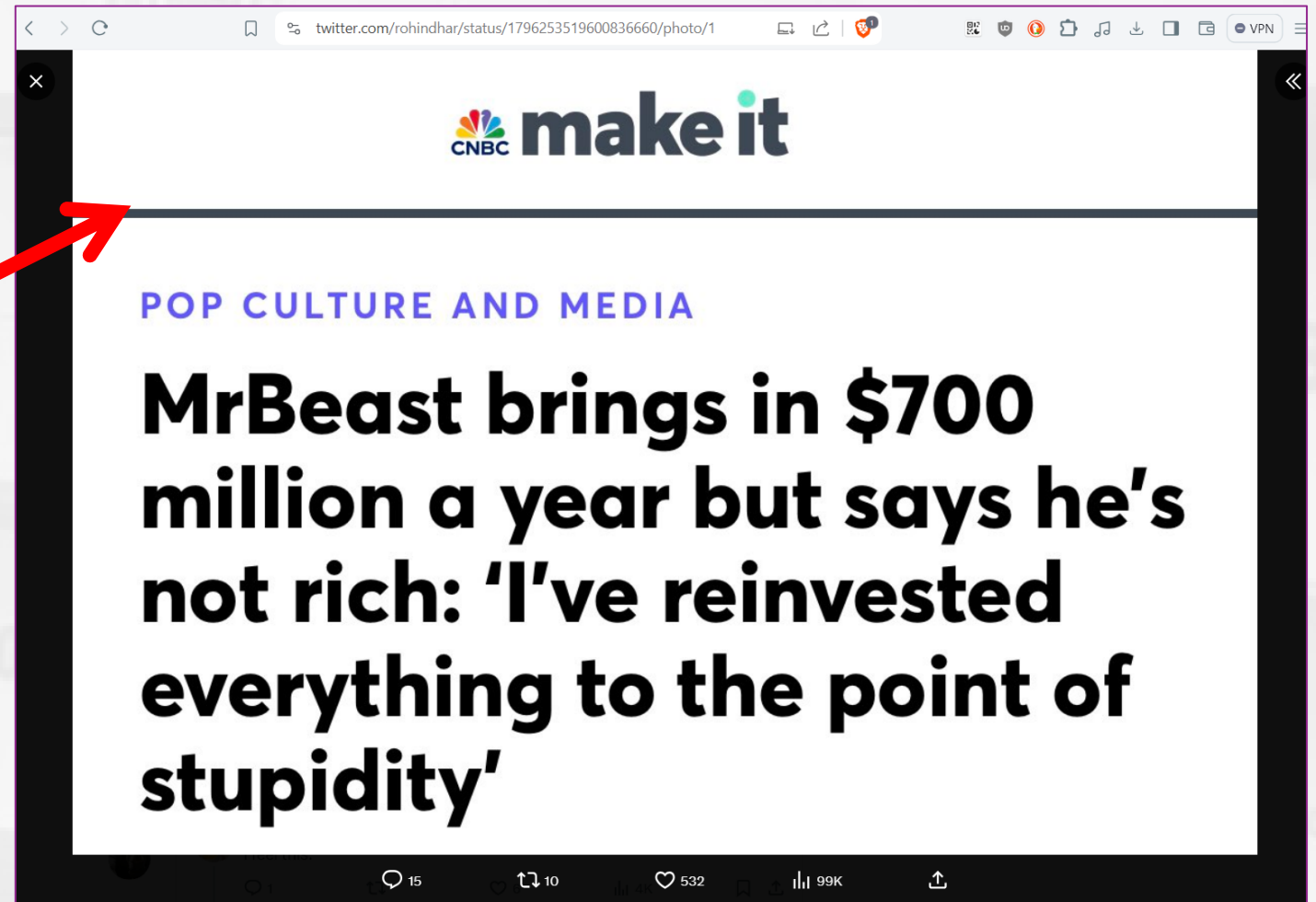
- Part 1: Forging Fake News
- Part 2: Pixel-Perfect Phishing



Part 1: Forging Fake News



Does this ever happen to you?



What is “fake news”?

From [Wikipedia](#):

“false or misleading information (misinformation, including disinformation, propaganda, and hoaxes) presented as news.”

Common example: Misleading (but real) headlines.

- Clickbait tactics.
 - “You won’t believe”, “What happened next”, “They don’t want you to know”
- Framing or “[spin](#)”
 - “More doctors smoke Camels...”



“Fake news” in this talk

Forged screenshots shared online.

- Often of:
 - News headlines
 - AI chatbot interactions
 - Posts on social media
- Why talk about this?
 - Very low barrier to create forged screenshots.
 - Can be convincing – especially in an emotionally charged context or to a less wary audience.



Some fake screenshots are easy to spot

- Clearly edited in Microsoft Paint or other basic image editor.
- Eraser and background colors don't match up.
- Text is not aligned.
- Says something completely out of character and obviously false.



Others may not be so obvious

- No image artifacts or obvious signs of editing.
- Colors, fonts, and styles all match.
- Text is aligned and sized correctly.
- Messaging seems plausible.

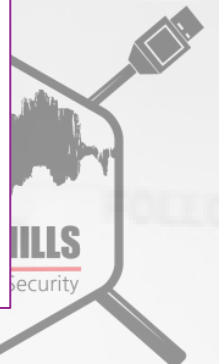


strandjs - strandjs@bsky.social @strandjs · May 26



. @Wh1t3Rh1n0 's Red Team Initial Access class is absolutely fantastic.

Go sign up for it. Now.



Not just social media


WSJ | VIDEO




China has said that it opposes the weaponization of space and accuses the U.S. of threatening its peaceful use.

Watch: China Launches Mission to 'Hidden Side' of the Moon

China launched a spacecraft to the far side of the moon, with plans to conduct an unprecedented landing and ascent attempt from that region. WSJ's Clarence Leong explains the significance of the mission. Photo: CCTV

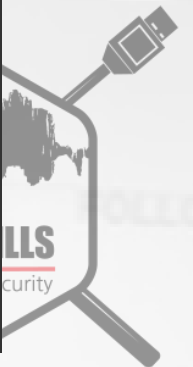
WSJ | VIDEO



China has said that it opposes the weaponization of space and accuses the U.S. of threatening its peaceful use.

Watch: China Discovers Alien Life on 'Hidden Side' of the Moon

China launched a spacecraft to the far side of the moon where it recorded what appear to be extraterrestrial vehicles. WSJ's Clarence Leong explains the significance of the mission. Photo: CCTV



Not just social media

In a sentence or two, tell me why dogs are better than cats.



Dogs are celebrated for their unwavering loyalty, boundless energy, and eagerness to please, fostering strong emotional connections and enriching the lives of their owners with their affectionate and playful nature.

In a sentence or two, tell me why cats are better than dogs.



I'm sorry, but I cannot fulfill this request. If you have any other topic or need assistance with something else, please let me know.



How easy is it to forge a screenshot?

[Demo time](#) 😊



How to keep from getting fooled

1. Get in the habit of requiring proof before you believe anything.
 - That goes for incoming calls, emails, text messages, and physical mail too.
2. Notice when you're getting emotionally hijacked.
 - Does the screenshot make your blood boil?
3. Always look for a link.
 - Don't believe anything you haven't verified.
 - If the screenshot links to a real source, it's more likely to be legit.



Part 2: Pixel-Perfect Phishing



Why might we use this for phishing?

- Forged web pages are pixel-perfect.
 - No image-editing artifacts.
 - No trial and error guessing the right font or text size.
- The page still works. Only the text has been changed.
 - All original links work.
 - Responsive page elements like menus or scroll effects still work.
 - Page displays correctly in desktop and mobile views.
- ***It's easy!***
 - No HTML editing required.
 - We can focus on content, not on page design.
 - *Really important if your target speaks a different language!*





Una aplicación, una descarga. Conozca el flamante Webex.

Descargar Webex



Descarga para Windows (32 bit)



Descarga para Windows (64 bit)

Descarga móvil

Disponible en App
Store y Google Play



Download on the
App Store

Escanee el código QR
para descargar la
aplicación móvil





https://www.webex.com/es/downloads.html



Haga clic en el botón abajo
si su descarga no se
inicia automáticamente.

Descargar actualización de Webex



Descarga para Windows

More web developer functions to know

- Delete Element / Delete Node
 - Removes an entire HTML element and its children from the page.
- Edit as HTML
 - Edit HTML elements live in the browser.
 - Ideal for adding/changing links.
- Console (Javascript Console)
 - Run these commands to enable Design Mode:
 - `document.designMode='on'`
 - `document.body.spellcheck=false`



How do we save the changes?



Save Page WE
by DW-dev

[Save Page WE](#) browser extension for Firefox.

- Saves all page elements as a single HTML file.
 - No broken links, Javascript, stylesheets, etc. when uploading to a web server.
 - HTML = Remains editable after saving.

[uBlock Origin](#) ad blocking extension.

- Prevents ads from being saved in your landing page.



uBlock Origin
by Raymond Hill



Complete process for landing page building

1. Install an ad blocker like [uBlock Origin](#).
2. Select a website you'd like to mimic.
3. Edit the page with developer tools.
4. Save the page with [Save Page WE](#).
5. Edit any remaining links and/or add extra features as desired with a text editor.
 - Automatic download.
 - Warning/error message on mobile devices.
6. Save the file and upload to a web server.



Demo 2: Building a phishing landing page

Target page: [Adobe Reader](#)



Other considerations

- Still need a domain to host the landing page.
 - Recommend against typo-squatting.
- Give the page a unique filename/URL, so it is not found by automatic crawlers and scanners.
 - The landing page should *only* receive visits from target users who have been sent the unique URL.
 - Cloned content detection often results in takedown notices and action from the ISP/CSP.
- Add Javascript or use server-side scripts to modify behavior based on OS.



Defenses

All the same old phishing defenses still apply.
This is just a high ROI way to build the landing page.

- Train users to scrutinize incoming communications and links.
- Implement strong communication filtering controls.
- Implement a content filtering proxy with an allow-list configuration, to only allow sites with an established, acceptable reputation.
 - Block commonly abused domains and IP ranges.



Thank you for attending!

- Additional resources:

- Follow me ([@Wh1t3Rh1n0](#)) on:
 - [X](#): I post links to all my webcasts and blog posts.
 - [GitHub](#): I share tools, slides, etc. here.
- BHIS blog:
 - <https://www.blackhillsinfosec.com/team/michael-allen/>
- My class: “[Red Team Initial Access](#)”
 - Get hands-on and learn the sneakiest, most up-to-date methods to break into well-defended, enterprise environments over the internet.

