



nmtcSM
Northeastern Maryland Technology Council

SCIENCE CAFÉ



TECHNOLOGY

STEM

VISIONARY AWARDS

ABOUT NMTC

EVENTS

DONATE

MEMBERSHIP

NEWS/PHOTOS

SPONSORSHIP

WATER COOLER – DIGITAL RESOURCES COMPROMISED?

Date/Time

Date(s) - 10/01/2020

4:00 pm - 5:00 pm

Category(ies)

Virtual Event

Water Cooler



October 01, 2020

“Were Your Digital Resources Compromise, Working Remotely?”

Register here: <https://us02web.zoom.us/meeting/register/tZMsd-ihpj0iG9DPc-GvCU5GyTLtNSJrgdLI>



Marco Ciavolino

- General Marketing Communications
- STEM training materials by RobotMats
- Web Development in JOOMLA and Wordpress
- Graphic Design/Corporate ID
- Photography/Video
- Tech Research & Development
- Founder of Techbrick Robotics
- Founder of RobotMats.com



<http://enktesis.com>

Darcy, the web cat.



Resources

After the talk we will send you the PPT and Word Document.



enktêsis
Are Your Digital Assets Compromised?
 Let's see if you can find your ID.
 Digital Resources Compromised
 Marco Ciavolino * www.enktesis.com * 410.838.8264

XCORP 2014 LLC *enktêsis
 XCORP2014/Enktêsis
 4 Newport Drive Site B
 Forest Hill, MD 21050
<http://enktesis.com>

WATER COOLER – DIGITAL RESOURCES COMPROMISED?

Friday, October 1, 4-5p

SPEAKER
 Marco Ciavolino runs a private consultancy, enktesis, LLC, that assists clients in a range of web technology solutions, marketing communications, business development, and communications research efforts. He has been involved in the web space, almost from its inception in the '90's, and since 1995 has directly developed and collaborated on hundreds of web projects from small niche sites to large enterprise projects.

TOPIC
 We rely ever more on our digital resources to work flawlessly, where the scramble to work remotely during Covid-19 has compromised, previously consistent, well structured, resources related to corporate identification, corporate information, and IT logins and resources. The sudden rush to work remotely have found these core, critical items cobbled together, with numerous versions and individual with logins and control that are unknown to the organization at large. How do we fix this? Our expert, who troubleshoots thousands of digital resources shares quick, "keep it safe" steps to return you and your organization to a digital strong structure.

Every client with whom I have worked cannot provide consistent, well structured, resources related to corporate identification, corporate information, and IT logins and resources. These are core, critical items that are often cobbled together, with numerous versions and individual with logins and control that are unknown to the organization at large. How do we fix this? Here the steps in a general order of importance.

Freed from the constraints of the office structure and accountability you may find that your digital assets have taken on a life of their own.

XCORP 2014 LLC *enktêsis
 XCORP2014/Enktêsis
 4 Newport Drive Site B
 Forest Hill, MD 21050
<http://enktesis.com>
 Page 2 of 8

is is a Dangerous Thing

| ITEM | COMMENTS | RESULTS |
|-------------------|---|---------|
| Password Strength | http://www.passwordmeter.com/ https://www.usa.edu/sdgs/strong-password/ https://www.comparitech.com/privacy-security/tools/password-strength-test | |
| Fingerprinting | https://www.amuniqua.org Device fingerprinting or browser fingerprinting is the systematic collection of information about a remote device, for identification purposes. Client-side scripting languages allow the development of procedures to collect very rich fingerprints: browser and operating system type and version, screen resolution, architecture type, lists of fonts, plugins, microphone, camera, etc. https://www.amuniqua.org/faq Even more scary data. http://browserspy.dk/ | |
| Phishing | What is Phishing? https://www.phishing.org/what-is-phishing Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss. | |
| Pwned | https://haveibeenpwned.com 'Pwn' is a lot like the sense of 'own' that means 'to have power or mastery over (someone)'. It has also been used to describe the act of gaining illegal access to something. https://www.merriam-webster.com/words-at-play/pwn-what-it-means-and-how-you-say-it | |

Are Your Digital Assets Compromised?

Let's see if you
can find your ID.



Are Your Digital Assets Compromised?

We rely ever more on our digital resources to work flawlessly, where the scramble to work remotely during Covid-19 has compromised, previously consistent, well structured, resources related to corporate identification, corporate information, and IT logins and resources. The sudden rush to work remotely have found these core, critical items cobbled together, with numerous versions and individual with logins and control that are unknown to the organization at large. How do we fix this? Our expert, who troubleshoots thousands of digital resources shares quick, “keep it safe’ steps to return you and your organization to a digital strong structure.



The first web cartoon:

“On the internet, nobody knows you’re a dog”

They also will not know if you are a viable business partner or vendor if you don’t tell them and show them in a competent manner.

https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog



THE LT. DAN RULE

Heed Lt. Dan in Forrester Gump:

“We have one rule here. Don’t do anything stupid like getting yourself killed.”

Are Your Digital Assets Compromised? The Big Issues

- Passwords/Authentication
- Digital Fingerprinting
- Pwnage
- Phishing



This is a dangerous thing.

Everyday Attacks

Home » Security Bloggers Network » Lockphish phishing attack: Capturing Android PINs & iPhone passcodes over https



Lockphish phishing attack: Capturing Android PINs & iPhone passcodes over https

by Howard Poston on September 30, 2020



5G IOT CLOUD AI SECURITY MO

MUST READ: [What is phishing? Everything you need to know to protect yourself from](#)

This worm phishing campaign is a game-changer in password theft, account takeovers

The security incident highlights the need for multi-factor authentication in the enterprise.

THREAT INTELLIGENCE

9/30/2020
01:50 PM



Phishing Attack Targets Microsoft 365 Users With Netflix & Amazon Lures

Cyberattacker TA2552 primarily targets Spanish speakers with messages that leverage a narrow range of themes and popular brands.



More ▾

Newsletters

Forums

Resource Library



Search

Join / Log In

Organizations facing nearly 1,200 phishing attacks each month

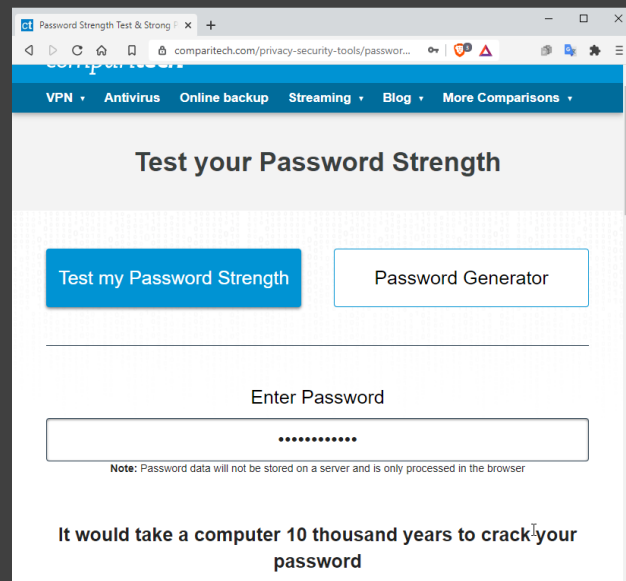
This is a dangerous thing.

Password Strength

- Employees balk at password changes.
- Testing Passwords.

<https://www.uic.edu/apps/strong-password>

<https://www.comparitech.com/privacy-security-tools/password-strength-test>



Test your Password Strength

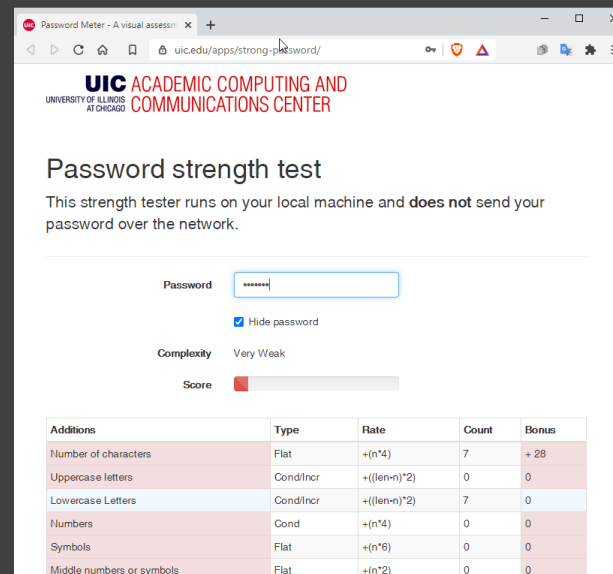
Test my Password Strength Password Generator

Enter Password

.....

Note: Password data will not be stored on a server and is only processed in the browser

It would take a computer 10 thousand years to crack your password



UIC ACADEMIC COMPUTING AND COMMUNICATIONS CENTER

Password strength test

This strength tester runs on your local machine and **does not** send your password over the network.

Password:

Hide password

Complexity: Very Weak

Score:

| Additions | Type | Rate | Count | Bonus |
|---------------------------|-----------|---------------------------|-------|-------|
| Number of characters | Flat | $+(n^4)$ | 7 | + 28 |
| Uppercase letters | Cond/Incr | $+\left((len-n)^2\right)$ | 0 | 0 |
| Lowercase Letters | Cond/Incr | $+\left((len-n)^2\right)$ | 7 | 0 |
| Numbers | Cond | $+(n^4)$ | 0 | 0 |
| Symbols | Flat | $+(n^6)$ | 0 | 0 |
| Middle numbers or symbols | Flat | $+(n^2)$ | 0 | 0 |

This is a dangerous thing.

Password Strength

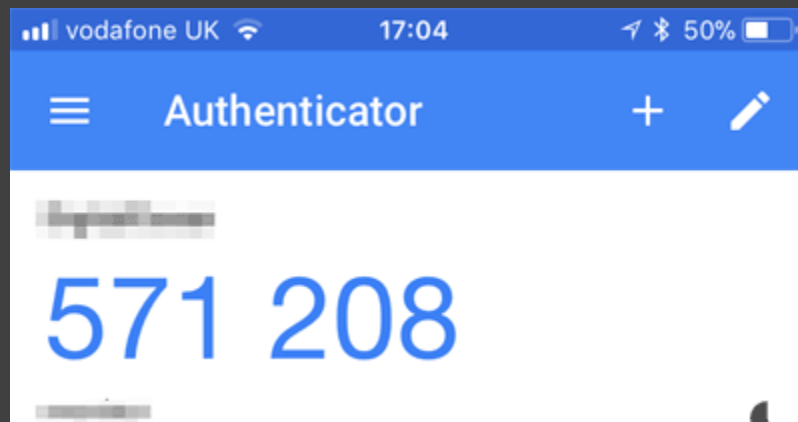
- **dec271969**
It would take a computer **3 hours** to crack your password
- **Dec#27!1969**
It would take a computer **2 thousand years** to crack your password
- **N33XCMewxbw3**
It would take a computer **10 thousand years** to crack your password

IMPORTANT: Hackers now routinely run through millions of known passwords from compromised databases (see Have I Been Pwned below.)

This is a dangerous thing.

Username/Passwords: What can you do?

- Identify Key Username / Password accounts.
- Test them for distribution.
- Update as necessary.
- Add third-party authentication.
- See being Pwned below.



This is a dangerous thing.

Fingerprinting

<https://www.amiunique.org>

Device fingerprinting or browser fingerprinting is the systematic collection of information about a remote device, for identification purposes. Client-side scripting languages allow the development of procedures to collect very rich fingerprints: browser and operating system type and version, screen resolution, architecture type, lists of fonts, plugins, microphone, camera, etc.

More info:

<https://www.amiunique.org/faq>

Even more scary data:

<http://browserspy.dk>



This is a dangerous thing.

Fingerprinting v. Cookies

Cookies

- Stores Settings
- No login required
- Can be blocked/deleted

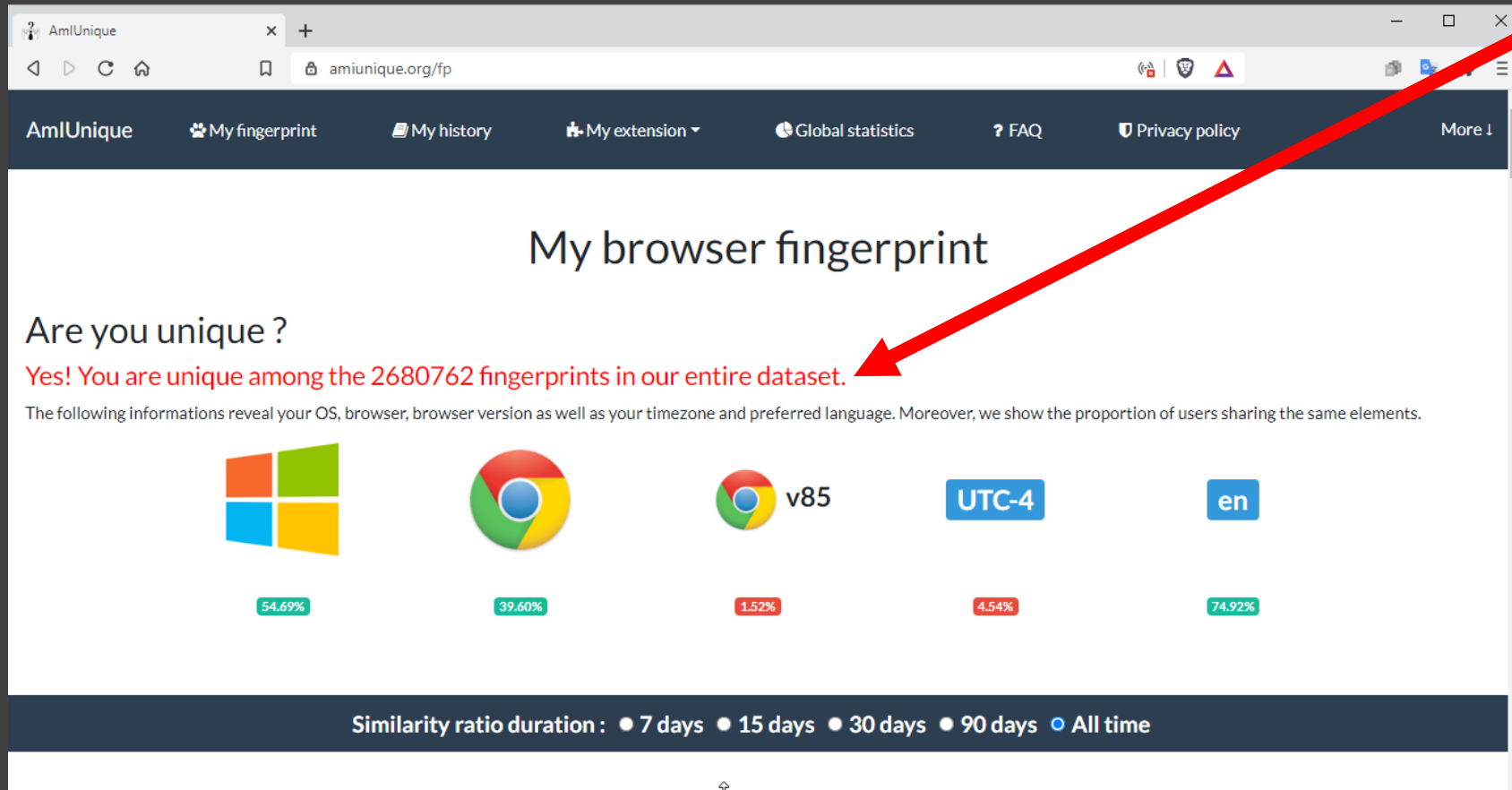
Finger Printing

- Records settings
- Any device, any level of security
- Behavioral analysis
- Live forever



This is a dangerous thing.

Fingerprinting



The screenshot shows a web browser window with the URL amiunique.org/fp. The page title is "My browser fingerprint". Below the title, it asks "Are you unique?" and provides a red confirmation: "Yes! You are unique among the 2680762 fingerprints in our entire dataset." A red arrow points to this text. Below this, it lists various browser and system attributes with their respective similarity percentages:

| Attribute | Similarity Ratio |
|----------------|------------------|
| Windows OS | 54.69% |
| Chrome Browser | 39.60% |
| Chrome v85 | 1.52% |
| UTC-4 Timezone | 4.54% |
| en Language | 74.92% |

At the bottom, there is a "Similarity ratio duration" selector with options for 7 days, 15 days, 30 days, 90 days, and All time (selected).

This is a dangerous thing.

Fingerprinting

More than 70
parameters
and 1400 sub
parameters.

user-agent
accept
accept-encoding
accept-language
upgrade-insecure-requests
referrer
userAgent-js
platform
cookies
timezone
languages-js
canvas
font-js
ad
doNotTrack
navigator_properties
buildID
product
productSub
vendor
vendorSub
hardwareConcurrency

javaEnabled
deviceMemory
plugins
screen_width
screen_height
screen_depth
screen_availTop
screen_availLeft
screen_availHeight
screen_availWidth
screen_left
screen_top
permissions
webGLVendor
webGLRenderer
webGLData
webGLParameters
storage_local
storage_session
storage_indexedDB
audioFormats
audioContext

analyserNode
audioData
videoFormats
mediaDevices
accelerometer
gyroscope
proximity_sensor
keyboard
battery
connection-js
key
locationbar
menubar
personalbar
statusbar
toolbar
result_state
font-flash
resolution-flash
language-flash
platform-flash

This is a dangerous thing.

Fingerprinting: What can you do?

- Read this Article: Browser Fingerprinting [2020 Update] – What Is It & How to avoid It
<https://blokt.com/guides/browser-fingerprinting>
- In the end, not much.
- Just be aware of the issue.

And educate your employees that they can always be uniquely tracked by everyone in the world. That is all.



This is a dangerous thing.

Been Pwned?

Pronounced 'powned.'

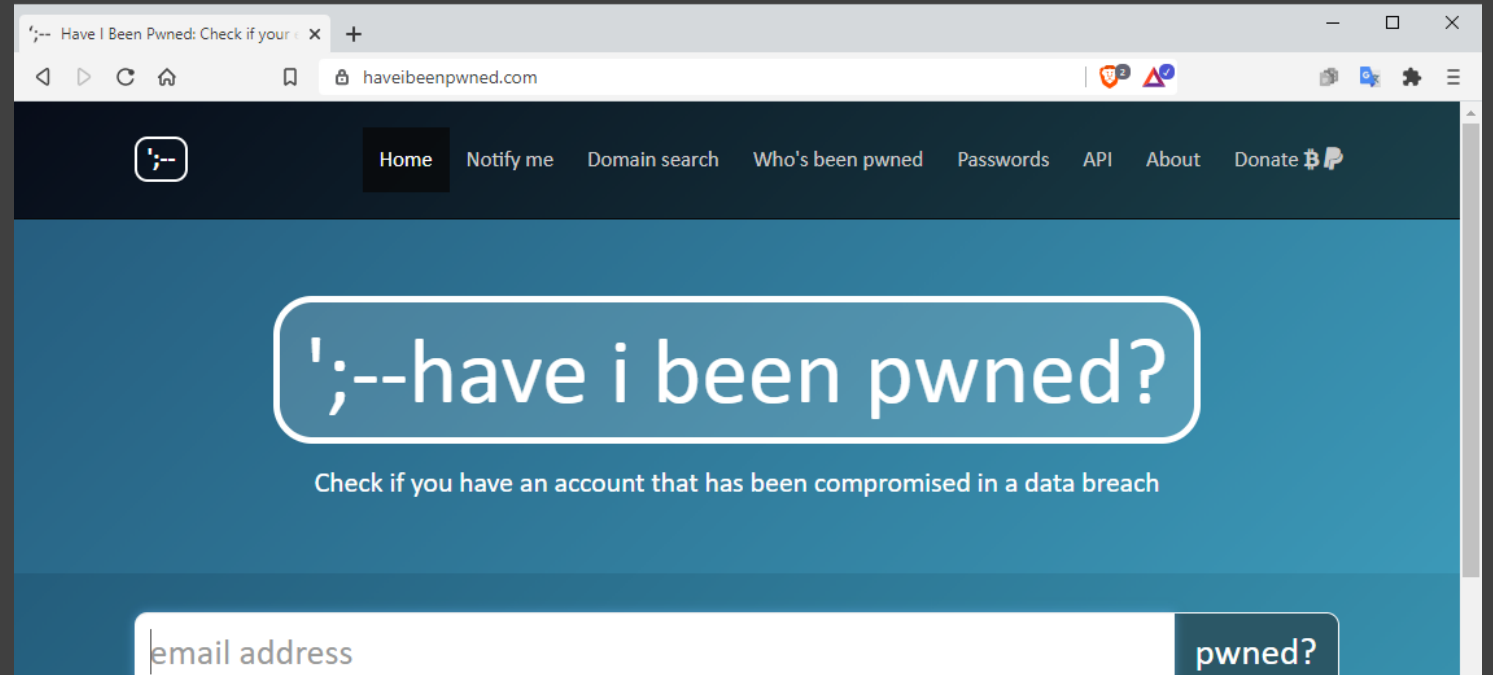
<https://haveibeenpwned.com/>

'Pwn' is a lot like the sense of 'own' that means "to have power or mastery over (someone)." It has also been used to describe the act of gaining illegal access to something.

Google Password Checker

<http://passwords.google.com>

(requires a gmail account)



479

pwned websites

10,196,051,455

pwned accounts

This is a dangerous thing.

Been Pwned?

Testing My Own Email
marco@enktesis.com

13 pwned sites.

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

500PX

500px: In mid-2018, the online photography community 500px suffered a data breach. The incident exposed almost 15 million unique email addresses alongside names, usernames, genders, dates of birth and either an MD5 or bcrypt password hash. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.in".

Compromised data: Dates of birth, Email addresses, Genders, Geographic locations, Names, Passwords, Usernames

APOLLO

Apollo: In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organisation.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles



B2B USA Businesses (spam list): In mid-2017, a spam list of over 105 million individuals in corporate America was discovered online. Referred to as "B2B USA Businesses", the list categorised email addresses by employer, providing information on individuals' job titles plus their work phone numbers and physical addresses. Read more about spam lists in HIBP.

Compromised data: Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses



Data & Leads: In November 2018, security researcher Bob Diachenko identified an unprotected database believed to be hosted by a data aggregator. Upon further investigation, the data was linked to marketing company Data & Leads. The exposed Elasticsearch instance contained over 44M unique email addresses along with names, IP and physical addresses, phone numbers and employment information. No response was received from Data & Leads when contacted by Bob and their site subsequently went offline.

Compromised data: Email addresses, Employers, IP addresses, Job titles, Names, Phone numbers, Physical addresses



Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

EXACTIS

Exactis: In June 2018, the marketing firm Exactis inadvertently publicly leaked 340 million records of personal data. Security researcher Vinny Troia of Night Lion Security discovered the leak contained multiple terabytes of personal information spread across hundreds of separate fields including addresses, phone numbers, family structures and extensive profiling data. The data was collected as part of Exactis' service as a "compiler and aggregator of premium business & consumer data" which they then sell for profiling and marketing purposes. A small subset of the exposed fields were provided to Have I Been Pwned and contained 132 million unique email addresses.

Compromised data: Credit status information, Dates of birth, Education levels, Email addresses, Ethnicities, Family structure, Financial investments, Genders, Home ownership statuses, Income levels, IP addresses, Marital statuses, Names, Net worths, Occupations, Personal interests, Phone numbers, Physical addresses, Religions, Spoken languages

JOOMLART

JoomlaArt: In January 2018, the Joomla! template website JoomlaArt inadvertently exposed more than 22k unique customer records in a Jira ticket. The exposed data was from Joomla and JomSocial, both services that JoomlaArt acquired the previous year. The data included usernames, email addresses, purchases and passwords stored as MD5 hashes. When contacted, JoomlaArt advised they were aware of the incident and had previously notified impacted parties.

Compromised data: Email addresses, Names, Passwords, Payment histories, Usernames

KICKSTARTER

Kickstarter: In February 2014, the crowdfunding platform Kickstarter announced they'd suffered a data breach. The breach contained almost 5.2 million unique email addresses, usernames and salted SHA1 hashes of passwords.

Compromised data: Email addresses, Passwords



Patreon: In October 2015, the crowdfunding site Patreon was hacked and over 16GB of data was released publicly. The dump included almost 14GB of database records with more than 2.3M unique email addresses and millions of personal messages.

Compromised data: Email addresses, Payment histories, Physical addresses, Private messages, Website activity



River City Media Spam List (spam list): In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

Compromised data: Email addresses, IP addresses, Names, Physical addresses



ShareThis: In July 2018, the social bookmarking and sharing service ShareThis suffered a data breach. The incident exposed 41 million unique email addresses alongside names and in some cases, dates of birth and password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by dehashed.com.

Compromised data: Dates of birth, Email addresses, Names, Passwords



Ticketify: In May 2018, the website for the ticket distribution service Ticketify was defaced by an attacker and was subsequently taken offline. The attacker allegedly requested a ransom to share details of the vulnerability with Ticketify but did not receive a reply and subsequently posted the breached data online to a publicly accessible location. The data included over 26 million unique email addresses along with names, physical addresses and phone numbers. Whilst there were no passwords in the publicly leaked data, Ticketify later issued an incident update and stated that "It is possible, however, that hashed values of password credentials could have been accessed".

Compromised data: Email addresses, Names, Phone numbers, Physical addresses



Verifications.io: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

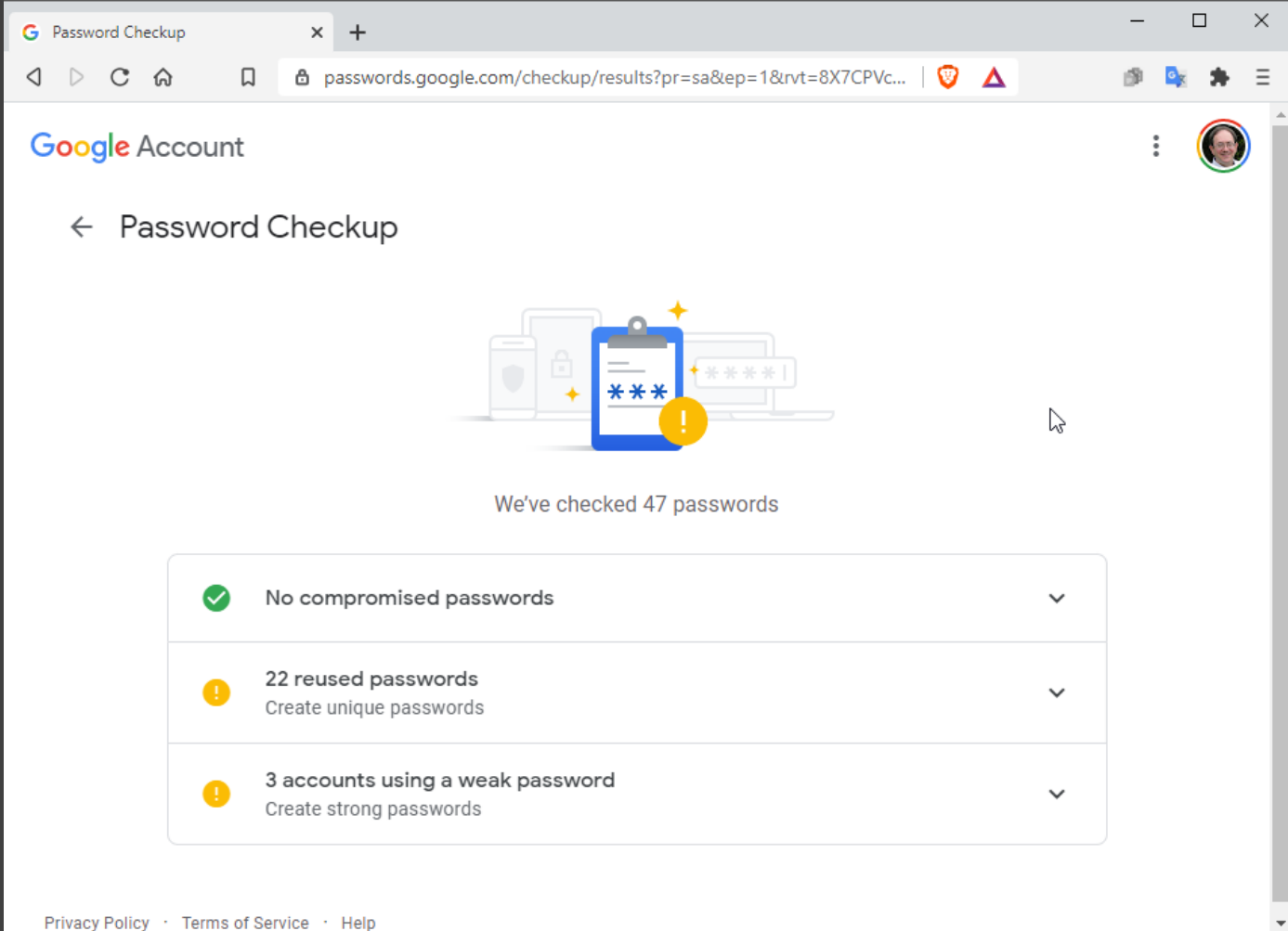
This is a dangerous thing.

Been Pwned?




Using Google Password Checker

<https://passwords.google.com/>

Looks at your stored passwords and gives you guidance.



The screenshot shows a web browser window with the URL `passwords.google.com/checkup/results?pr=sa&ep=1&nvt=8X7CPVc...`. The page title is "Password Checkup" and it displays the Google Account logo. The main heading is "Password Checkup" with a back arrow. Below the heading is an illustration of a smartphone, a laptop, and a clipboard with a password field containing asterisks and a yellow warning icon. The text "We've checked 47 passwords" is displayed. The results are shown in a list:

-  No compromised passwords
-  22 reused passwords
Create unique passwords
-  3 accounts using a weak password
Create strong passwords

At the bottom of the page, there are links for "Privacy Policy", "Terms of Service", and "Help".

This is a dangerous thing.

Been Pwned? What can you do?

- Test all key emails.
- Remove unused emails.
- Update all passwords.
- Add third-party authentication.

Ignore pwnage at your own risk.

The hackers will be happy.



This is a dangerous thing.

Phishing

<https://www.phishing.org/what-is-phishing>

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Nearly every major compromise has been used social hacking and phishing as the gateway to the final action.



This is a dangerous thing.

Phishing

In the news everyday.

One click can destroy your company.

Hacker steals \$15M after degens pile into unreleased Yearn Finance project

Cointelegraph · 22 hours ago



Foreign Hacker Sentenced in \$1M Scam Targeting Federal Employees and Contractors

Nextgov · Yesterday



These hackers have spent months hiding out in company networks undetected

ZDNet · 12 hours ago



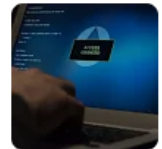
CISA says a hacker breached a federal agency

ZDNet · 5 days ago



Hackers Have Infiltrated Many of Washington State's Agencies

Bloomberg · Yesterday



This is a dangerous thing.

Phishing: Vectors

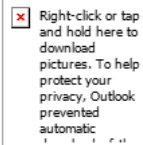
- Email itself.
- Email links.
- Phone calls.
- Scripts embedded in:
 - ✓ Word Documents
 - ✓ PDFs
 - ✓ Excel documents
 - ✓ Power Point Files
 - ✓ Some graphic formats (JPG headers)

They just need one entry point to infiltrate.



Microsoft Outlook interface showing an email from 'Order Shipment <care@amazn-ussshipment2.co>' to 'marco@techbrick.com' dated 'Thu 10/1/2020 10:03 AM'. The subject is 'Your prime order of iPhone 11 (64GB) worth \$749.99...'. The email content includes an order confirmation for order # 847-99857-167671711644, a greeting to 'marco@techbrick.com', and shipping information: 'Arriving: Saturday, October 03' and 'Your shipping speed: Two -Day Delivery'. The order will be sent to 'Mike S, Houston, Texas, US'.

Order summary
 Order #847-99857-167671711644
 Placed on Thursday, October 01, 2020

| | | |
|--|---|------------------|
| <div style="border: 1px solid gray; padding: 2px;">  </div> | iPhone 11 (64Gb, Purple) [Unlocked] Electronics Condition: New Sold by: NetworkStore Fulfilled by NetworkStore | \$749.99 |
| Item Subtotal: | | \$ 749.99 |
| Shipping & Handling: | | \$ 0.00 |
| Order Total: | | \$ 749.99 |

If you use a mobile device, you can receive notifications about the delivery of your package and track it from our free app.

We hope to see you again soon.

This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.

This is a dangerous thing.

Phishing: What can you do?

- Use an effective email firewall.
 - ✓ Included with Microsoft Live365, Google Business, Rackspace and others.
 - ✓ Be sure it is configured correctly.
- Use hardware firewalls.
- Use effective machine and device level software.
- Provide training to all staff and anyone with access to your systems to help them identify suspicious email.

One click can destroy your company.



This is a dangerous thing.

Phishing: What can you do ‘the sequel’?

- Setup and or confirm that you have **rigorous and complete backups** of all data and systems both local and remote
- **Demand** IT staff or consultants demonstrate a full **recovery**.
- Make sure someone in-house is **aware of the process**.
- **Keep up-to-date lists** of hardware and software requirements and active sources for equipment.



How long could you afford to be out of business?

Are Your Digital Assets Compromised?

Three other key areas.

- **Corporate ID Elements and Resources**
- **General Information Gathering**
- **Training, Training, Training.**



Corporate ID

| ITEM | COMMENTS |
|---------------------------------------|---|
| Logos | Must have key formats: * Illustrator, * eps, * Various raster forms |
| Colors | Established and defined in RGB/CMYK/PMS/HEX |
| Usage Guidelines | Where and how. Above below. Space around. Background. Sizes. |
| Phrases and punctuation. | Capitalization. Commas. Apostrophes. |
| Purging old versions of digital files | DOC, XLS, PDF, Images, Videos. |
| Publication Standards | Format, Size, Color, Binding, Distribution. |
| Reviewing publications | All print and digital. |
| Purging old versions of publications | Good luck. |
| Checking Digital Assets | Where is it stored. Is it accessible. |

IT Assets

| ITEM | COMMENTS |
|--|--|
| Do a username/account sweep. | Require a full test of UN/PW, Make Changes, Require Updates, Add Third-Party Authentication if Required. |
| Functional Email v Personal Emails | Review emails for receipt. Functional v. Personal. |
| Confirm a list of all online accounts | You will be surprised at how many there are. |
| Login to every account and check settings. | Update or delete. |
| Access to Critical Accounts | Corporate Email, Online backups, Domains and Domain registrars, Network Logins, Who, how, where. |
| Social Media Logins | Facebook (many users), Google Assets, Twitter, Linked In, etc. |
| Get confirmation on all software patches. | The primary vector for hacks is outdated software. |

Training

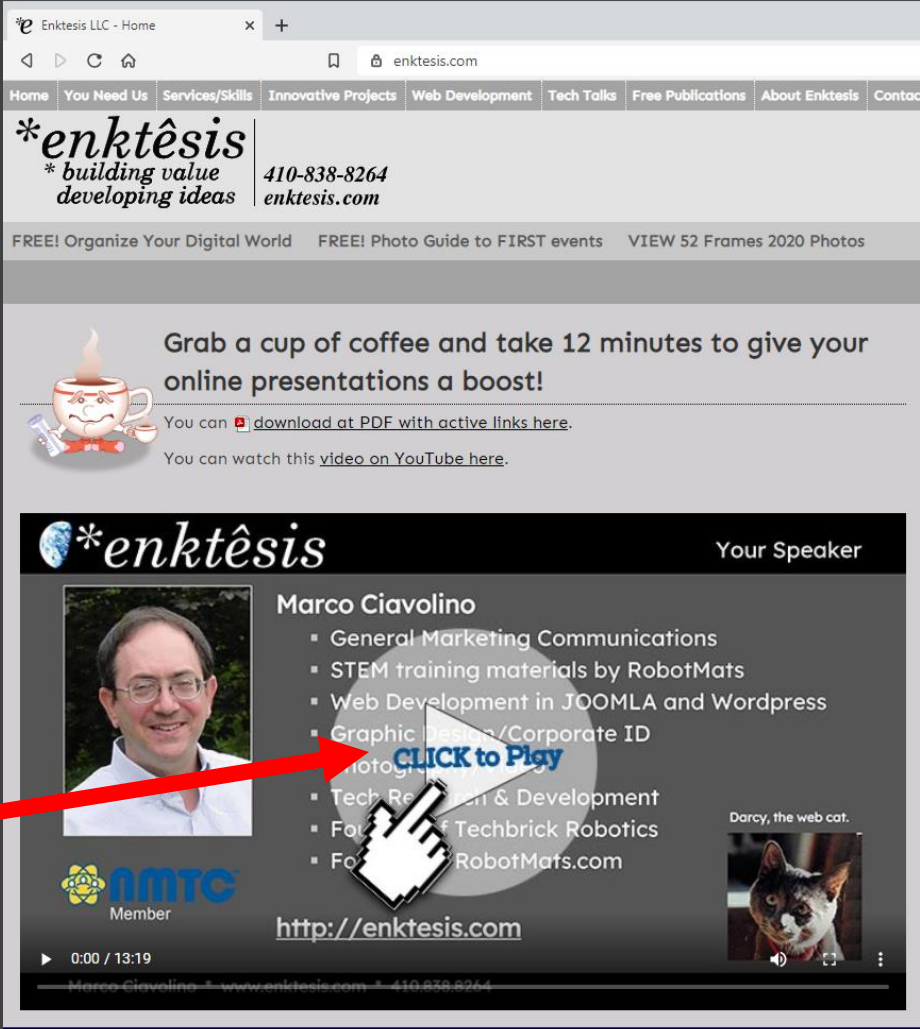
| ITEM | COMMENTS |
|-----------------------|-----------------------------------|
| Username/Passwords | Management, Updates, Protection. |
| Phishing | Awareness, Process for Reporting. |
| Security Protocols | Secure VPN, Secure workstations. |
| Use of Company Assets | Where, how, who to ask. |

Resources

Meetings...

<http://enktesis.com>

Improve Online Meetings



The screenshot shows a web browser window with the URL enktesis.com. The website header includes a navigation menu with items like Home, You Need Us, Services/Skills, Innovative Projects, Web Development, Tech Talks, Free Publications, About Enktesis, and Contact. The main content area features a promotional message: "Grab a cup of coffee and take 12 minutes to give your online presentations a boost!" with links to download PDFs and watch a video on YouTube. Below this is a video player for Marco Ciavolino, titled "Your Speaker". The video player includes a list of topics: General Marketing Communications, STEM training materials by RobotMats, Web Development in JOOMLA and Wordpress, Graphic Design/Corporate ID, Tech Research & Development, and Techbrick Robotics. A red arrow points to a "CLICK to Play" button over the video player. The video player also shows the AMTC Member logo and the website URL <http://enktesis.com>.

Resources

...A Lifetime of Ideas

<http://enktesis.com>

Organize Your Digital World

The screenshot shows a web browser window at enktesis.com/pubmenuorg. The navigation bar contains links for Home, You Need Us, Services/Skills, Innovative Projects, Web Development, Tech Talks, Free Publications, About Enktesis, and Contact. The main content area features a 'Publications' section with a list of items, including 'Secrets to organizing your digital world. No clearance required. [v_20170220]'. A red arrow points to a link in the navigation bar that has been replaced with a search bar, indicating a compromise of the original resource.

Enktesis LLC - FREE! Organize Your World

enktesis.com/pubmenuorg

Home You Need Us Services/Skills Innovative Projects Web Development Tech Talks Free Publications About Enktesis Contact

***enktesis**
** building value
developing ideas* 410-838-8264
enktesis.com

FREE! Organize Your Digital World FREE! Photo Guide to FIRST events VIEW 52 Frames 2020 Photos

Search ... Search

Publications

- Make Your Own Photobooth
- Photo Guide for FIRST Events and Other STEM Competitions
- Secrets to organizing your digital world. No clearance required. [v_20170220]

Secrets to organizing your digital world. No clearance required. [v_20170220]

CLICK HERE TO REQUEST A FREE COPY OF THIS USEFUL GUIDE

It will be emailed to you as an attachment. Why? Because we are updating these documents all the time and we want to keep you up to date!

INCLUDES

- Opening Page 1
- Introduction 2
- FIVE IMPORTANT BUSINESS PRINCIPLES 3
- FILE NAMING SO YOU CAN FIND YOUR WORK 4
- FOLDER NAMING AND VERSIONING 5
- A MOST EXCELLENT TIP FOR OUTLOOK PART 1 6
- E-COMMERCE IS HARD: No Magic Bullets 7
- FORMAT YOUR EMAIL IN A SENSIBLE MANNER 8
- DON'T SEND TO, CC OR BCC WHEN YOU SHOULD SEND PERSONALLY 9
- NITTY GRITTY OF WEBSITE DEVELOPMENT 10



Marco Ciavolino

- General Marketing Communications
- STEM training materials by RobotMats
- Web Development in JOOMLA and Wordpress
- Graphic Design/Corporate ID
- Photography/Video
- Tech Research & Development
- Founder of Techbrick Robotics
- Founder of RobotMats.com



<http://enktesis.com>

Darcy, the web cat.





<http://nmtc.org>

The NMTC (Northeastern Maryland Technology Council) is the technology and innovation advocacy platform providing expert opinions, on disruptive technologies, affecting Revenue, Talent and Technology Pipelines of our members in Northeastern Maryland, the Greater Baltimore area and beyond.

Join Today!