COMPUTER & INTERNET BASICS FOR SENIORS

Agenda

Keeping you and your device safe

Building confidence

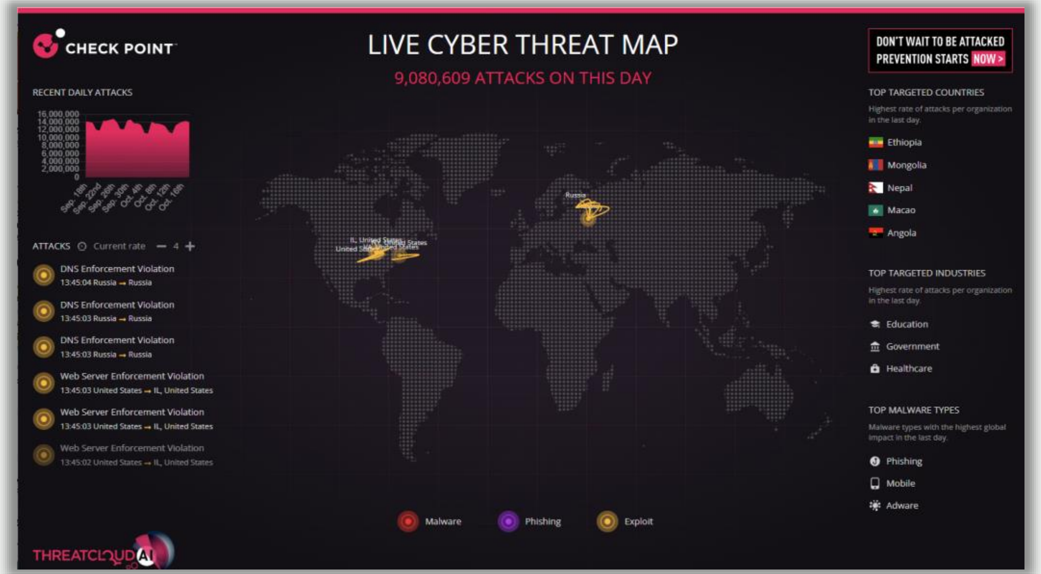
Engaging the social media frenzy

What to do in an emergency

Final tips & takeaways

World Maps of Live Threats

Click each map to see real-time threats.



CHECK POINT

LIVE CYBER THREAT MAP

9,080,609 ATTACKS ON THIS DAY

DON'T WAIT TO BE ATTACKED PREVENTION STARTS NOW >

RECENT DAILY ATTACKS

ATTACKS Current rate — 4 +

DNS Enforcement Violation
13:45:04 Russia → Russia

DNS Enforcement Violation
13:45:03 Russia → Russia

DNS Enforcement Violation
13:45:03 Russia → Russia

Web Server Enforcement Violation
13:45:03 United States → IL, United States

Web Server Enforcement Violation
13:45:03 United States → IL, United States

Web Server Enforcement Violation
13:45:02 United States → IL, United States

TOP TARGETED COUNTRIES
Highest rate of attacks per organization in the last day.

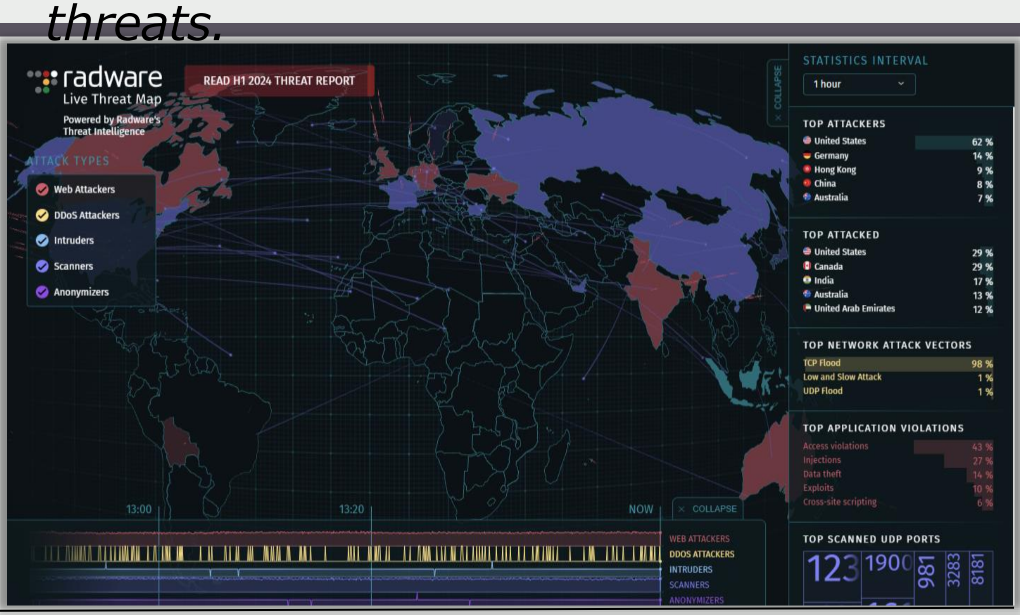
- Ethiopia
- Mongolia
- Nepal
- Macao
- Angola

TOP TARGETED INDUSTRIES
Highest rate of attacks per organization in the last day.

- Education
- Government
- Healthcare

TOP MALWARE TYPES
Malware types with the highest global impact in the last day.

- Phishing
- Mobile
- Adware



radware
Live Threat Map
Powered by Radware's Threat Intelligence

READ H1 2024 THREAT REPORT

ATTACK TYPES
- Web Attackers
- DDoS Attackers
- Intruders
- Scanners
- Anonymizers

STATISTICS INTERVAL
1 hour

TOP ATTACKERS

United States	62 %
Germany	14 %
Hong Kong	9 %
China	8 %
Australia	7 %

TOP ATTACKED

United States	29 %
Canada	29 %
India	17 %
Australia	13 %
United Arab Emirates	12 %

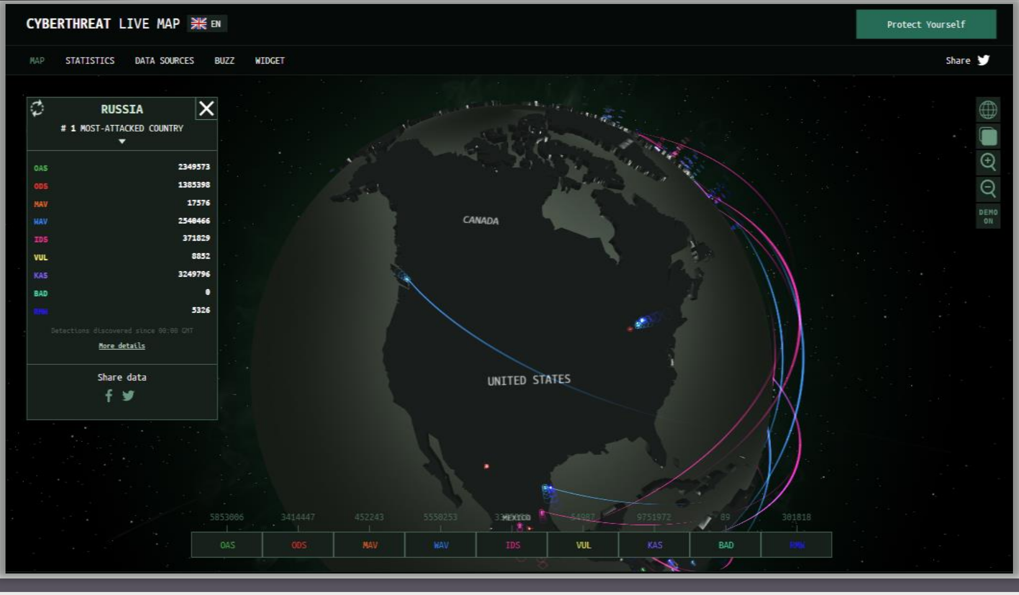
TOP NETWORK ATTACK VECTORS

TCP Flood	98 %
Low and Slow Attack	1 %
UDP Flood	1 %

TOP APPLICATION VIOLATIONS

Access violations	43 %
Injections	27 %
Data theft	14 %
Exploits	10 %
Cross-site scripting	6 %

TOP SCANNED UDP PORTS
123 1900 981 3283 8181



CYBERTHREAT LIVE MAP EN

Protect Yourself

MAP STATISTICS DATA SOURCES BUZZ WIDGET Share

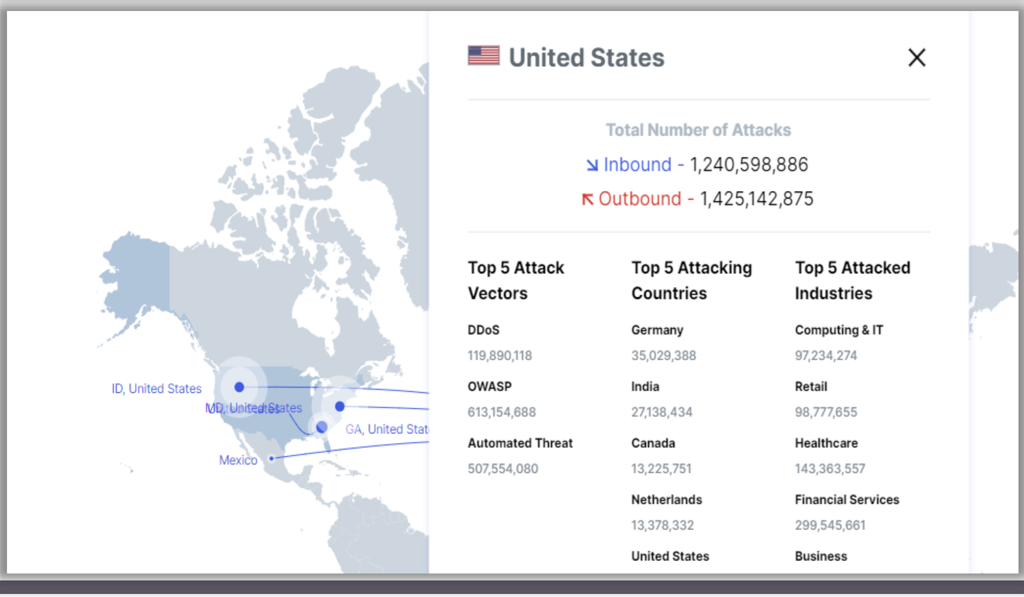
RUSSIA
1 MOST-ATTACKED COUNTRY

OAS	2349573
ODS	1385398
MAV	17576
WAV	2540466
IDS	371829
VUL	8852
KAS	3249796
BAD	0
RMW	5326

Detections discovered since 00:00 GMT

More details

Share data



United States

Total Number of Attacks
↘ Inbound - 1,240,598,886
↖ Outbound - 1,425,142,875

Top 5 Attack Vectors	Top 5 Attacking Countries	Top 5 Attacked Industries
DDoS 119,890,118	Germany 35,029,388	Computing & IT 97,234,274
OWASP 613,154,688	India 27,138,434	Retail 98,777,655
Automated Threat 507,554,080	Canada 13,225,751	Healthcare 143,363,557
	Netherlands 13,378,332	Financial Services 299,545,661
	United States	Business

THE POWER OF PROTECTION

Knowing your device will allow you to keep it safer to use and enjoy more.

Overcoming nervousness

Confidence-building strategies

Engaging with your Social Media Sites

Being social media savvy will be in your best interest! Here are some tips to help you:

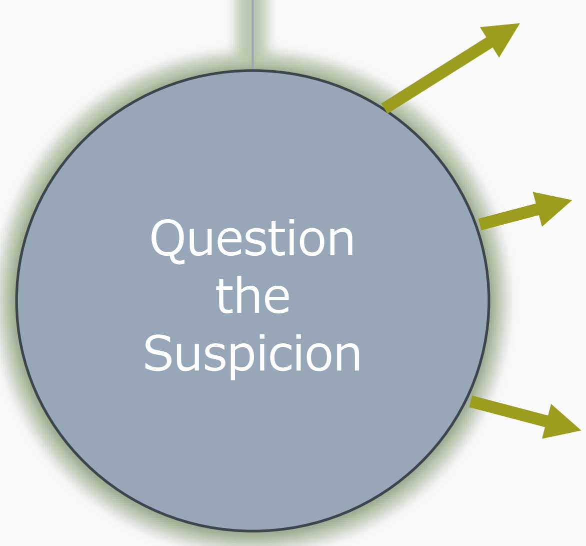
- **Beware of strangers** trying to “friend” you or who ask you for money. Block these people immediately.
- **Never click on links from strangers** or go to websites they want you to go to as they are most likely fraudulent.
- **Unfriend or block anyone you don’t know** in your friend’s list.
- **Always log off sites when you are finished** with them.
- **Alert other family members** of what is going on, or the authorities if you are being threatened, extorted, or harassed online.

Be alert and vigilant when gaming!

Games may be fun but behind the scenes…beware!

Common online threats include:

- ✓ **Viruses** (Malicious programs designed to wreak havoc on your devices.)
- ✓ **Malware** (Software designed to damage a computer, steal data, or financially exploit unsuspecting users)
- ✓ **Phishing** (Creating fake websites, phone numbers, or email addresses that mimic legitimate sources)
- ✓ **Privacy breaches** (The release of personal information (such as email addresses, usernames, passwords, and even credit card numbers and social security numbers) to the public and dark web servers.)
- ✓ **Fraud and scams** (Targeting your vulnerabilities or unknowingness about them.)



Question the Suspicion

"Why is someone asking me to download a file?"

"How did I win a sweepstakes that I never entered?"

"Why are they asking for my social security number or my bank account number?"

- If you go to an unsafe site, the best thing to do is to immediately close that tab and exit your browser window.
  - You can also clear browsing history
  - You can set that site as unsafe so the browser will remember and warn you if go there again.

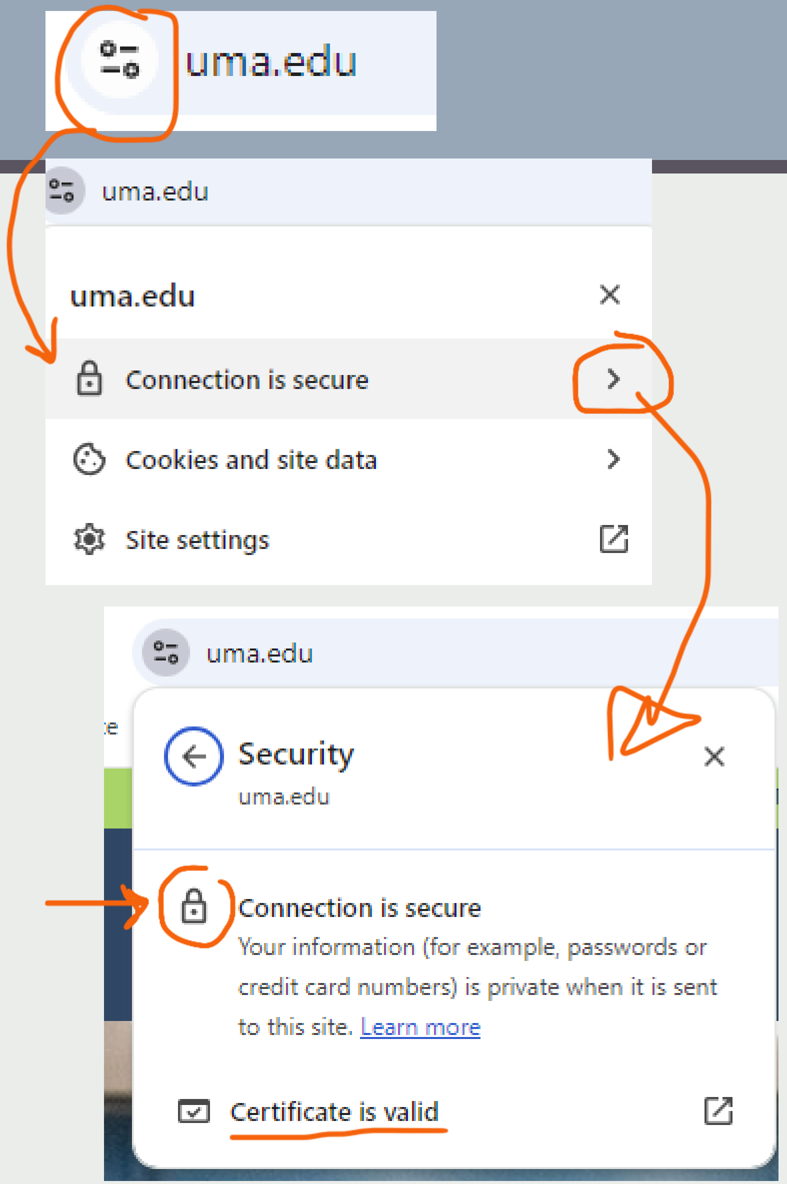
How to use your Browser settings:

Look for the 3 dots in the upper right corner of your browser (⋮).

Click on ***History*** and then “***Delete browsing Data***”. When the *Delete browsing data* dialog box appears, make sure the time range box says, “*all time*” and then click the **Delete data** button on the lower right corner.

Tip: (Ctrl + Shift + Del is a shortcut to open the dialog box.)

The best defense is being proactive!



Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

How to know if a site is secure

Click on the web address (e.g., www.uma.edu) and then the little icon that will appear to the left of it.

Clicking the icon will give you a drop-down menu of the site’s security. You can click the arrow on the right of the “Connection is secure” to see more information and whether the site has a valid certificate or not.

Clicking on the “Cookies and site data” arrow will allow you to manage on-device site data and to delete unwanted cookies.

Preventing yourself from going to unsafe sites:

Go to the three dots (⋮) in the upper right corner of your browser and click on ***Settings***.

Click ***Privacy and security*** from the left side menu. Then click ***security*** from the middle menu.

Scroll down to *Secure connections* and make sure it is turned on.

- If you are unsure whether a site is safe or not, you probably shouldn’t be there.
- Look for the padlock to the left of the web address.

Remember the word

S.A.F.E.

S: secure device

A: always protect yourself

F: follow safe browsing protocols

E: ensure you have strong passwords

Strong Passwords Tips		Good Password Example:
Use phrases you can remember; use a favorite saying or quote.	Think of a passphrase you can remember	**Fløw3RSr4m@** (flowers are for me) or **R3d*I5#myf@v3** (Red is my fave color)
Never use simple words anyone can guess!	**No** to words like: P@sswørd1 or Password or Pass123	**Ilik3FløWer3s*** (I like flowers) or **Turn)FF8c24@9pm** (Turn off PC at 9 pm)
Create a password that is at least 8 characters long!	Add numbers, letters and symbols	**L@ur3n24*1** or **Fløw3r5@re4m***
Change your password regularly!!	Change password if you think your account has been compromised, or if they have not been changed in over 3 months.	

BEING S.A.F.E. MINIMIZES YOUR ONLINE VULNERABILITY AND RISK!

WHAT TO DO IN AN EMERGENCY

#1 thing you can do is remain calm and reach out to someone trustworthy for help!

Final tips & takeaways

HOW TO KEEP YOURSELF SAFE AND PREVENT YOUR DEVICE FROM GETTING ATTACKED:

- **Protect yourself from malware**
  - Install Antivirus software on your devices
  - Only visit safe websites
- **Protect yourself from phishing scams**
  - Don’t click on suspicious links or ads
- **Communicate to others**
  - Let others know so they can help you
  - Don’t be intimidated or afraid to ask for help
- **Keep your devices up-to-date**
  - Install system updates when they become available
  - Back up your data regularly

THANK YOU

Dr. Lauren Mayhew, DCS

Assistant Professor of Computer Science and Cybersecurity