

Taking Action: How to safely shop online on Cyber Monday

POSTED 10:41 PM, NOVEMBER 30, 2014, BY [CHRISTINE KILLIMAYER](#)

 FACEBOOK TWITTER REDDIT PINTEREST LINKEDIN EMAIL

This is an archived article and the information in the article may be outdated. Please look at the time stamp on the story to see when it was last updated.

Please enable Javascript to watch this video

HUNTSVILLE, Ala. (WHNT) - Every year more and more people choose to avoid the hoards of holiday shoppers and buy online. With Cyber Monday set for December 1, 2014, cyber criminals are also gearing up for the Christmas rush.

According to [Enigma Software Group](#), on the three days surrounding Cyber Monday 2013, malware infections spiked more than seven percent in Huntsville and 40 percent nationally. Experts say you can expect the same this year.

"Malware authors are really trying to write their software to target as many people as possible," said Enigma Software Senior Vice President of Technology Patrick Morganelli.

Email driven scams are the most popular and PC users are the most susceptible. If you receive an email from a company with a link to a deal that seems too good to be true, it probably is.

"When the user clicks these malicious links, they'll often be redirected to a website which will download and install malware on their computer, which can really ruin their holidays," said Morganelli.

Links received through social media, even from those you know, can also be just as risky. Instead, do the leg work to verify the offer.

"Instead of clicking in links blindly in the email, actually go to the website that claims to have sent the email and if the deal is real, it will be on their real website," said Morganelli.

To truly insure your online safety have anti-malware software, such as SpyHunter, installed and make sure to run frequent scans and updates.

The Birmingham FBI Field Office also warned shoppers to beware of cyber criminals and their aggressive and creative ways to steal money and personal information.

The office offered these tips to help you avoid becoming a victim of cyber fraud:

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mails claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders. Always run a virus scan on attachment before opening.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the web address link you are directed to and determine if they match.
- Log on directly to the official website for the business identified in the e-mail, instead of "linking" to it from an unsolicited e-mail. If the e-mail appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.
- Contact the actual business that supposedly sent the e-mail to verify that the e-mail is genuine.
- If you are requested to act quickly or there is an emergency, it may be a scam. Fraudsters create a sense of urgency to get you to act impulsively.
- If you receive a request for personal information from a business or financial institution, always look up the main contact information for the requesting company on an independent source (phone book, trusted Internet directory, legitimate billing statement, etc.) and use that contact information to verify the legitimacy of the request.
- Remember if it looks too good to be true, it probably is.



POPULAR



Local West End Grill employees risk their lives to save tenants in early morning Huntsville apartment fire



HPD charges 3 with Capital Murder in toddler's shooting death



1 student dead, another injured following accidental Birmingham school shooting

LATEST NEWS



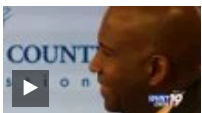
The Latest: Nepal police say at least 38 dead in plane crash



Early morning fire destroys storage shed behind North Ridge Apartments club house



Large tree falls, blocks part of Bankhead Parkway, driver involved uninjured



Newly appointed Madison County Commissioner is "ready to serve"



Spotify®

Spotify Plagued by Tech Support Scammers



HiWAAY Alerts Users of Recent Phishing Attempts



Google Chrome Users – Beware!



Huntsville to get new school for cyber technology and engineering



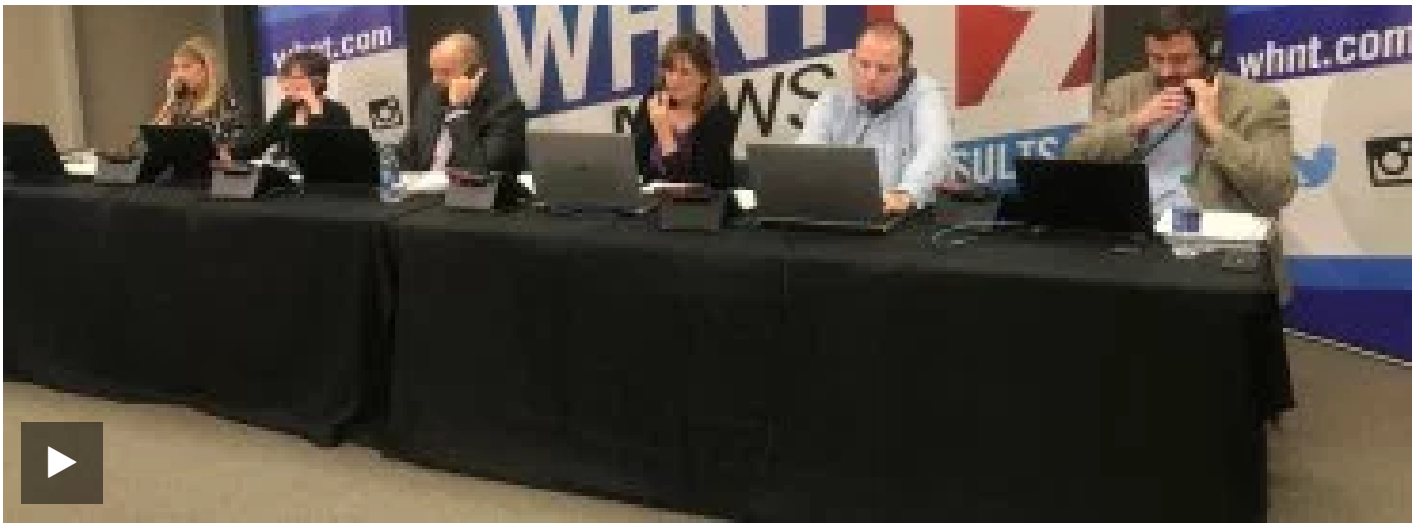


Watch Out for “Scarab”: It Comes in Sheep’s Clothing!



New Scam Targets Netflix Users





WHNT's annual Tax Action Line helps over a hundred people get answers



PlayStation 4 update lets parents boot kids from playing





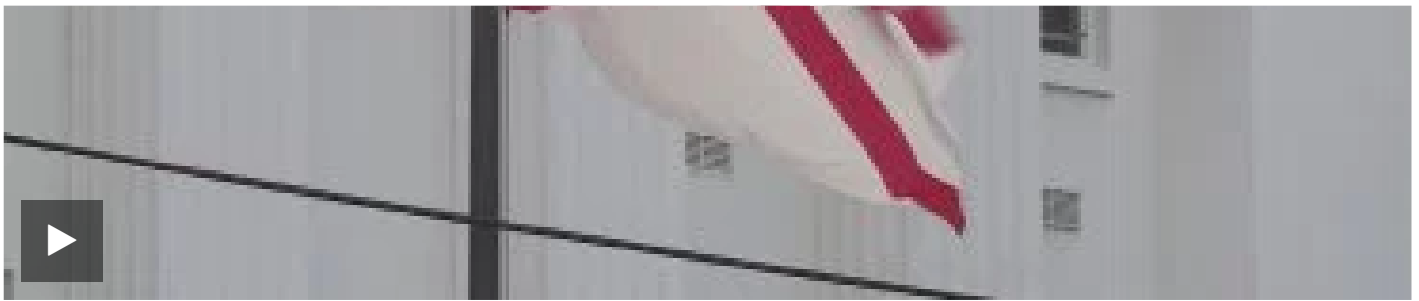
How young is too young for a child to have a cellphone?



A local 'cyber security evangelist' reflects on 2017's personal information hacks



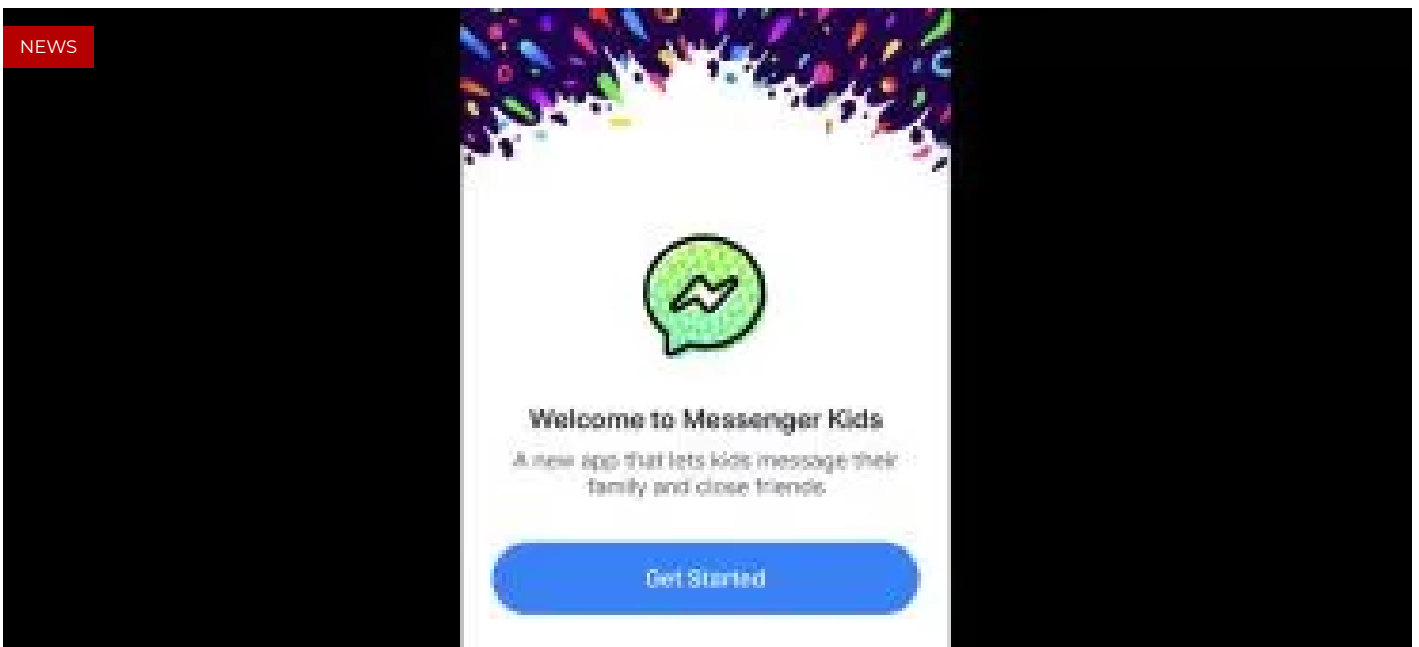
HUNTSVILLE • POLITICS



As Legislative session begins, business leaders have high goals for growth



Is Facebook listening in on your conversations?





Child experts: Just say 'no' to Facebook's kids app

MOBILE APPS

[IPHONE & IPAD APP](#)

[ANDROID APP](#)

[LIVEALERT19 WEATHER APP](#)



[FACEBOOK](#)



[TWITTER](#)



[EMAIL ALERTS](#)



[ABOUT & CONTACT](#)



[COVERS](#)

[ONLINE PUBLIC FILE](#) · [TERMS OF SERVICE](#) · [PRIVACY POLICY](#)

· 200 HOLMES AVENUE, HUNTSVILLE, AL 35801

· COPYRIGHT © 2018, WHNT

· A TRIBUNE BROADCASTING STATION · POWERED BY WORDPRESS.COM VIP