FAYCPD.COM

CONSUMER PROTECTION DIVISION

MONTHLY NEWSLETTER

ISSUE 7| JULY 2024

TRENDING TOPICS

- Beware of Senior Citizens Scams: Essential Tips to Safeguard Yourself or Loved Ones
- Job Related Scams are on the Rise in North Carolina
- Exposing the Underbelly: Common Scams Targeting Small Businesses
- No-Cost Advertisement Opportunity for CPD Certified Businesses
- Tell Us Your Story: Promotional Opportunity

Major Trending Scams Target Individuals Ages 55+ : How This Impacts Your Business & Family

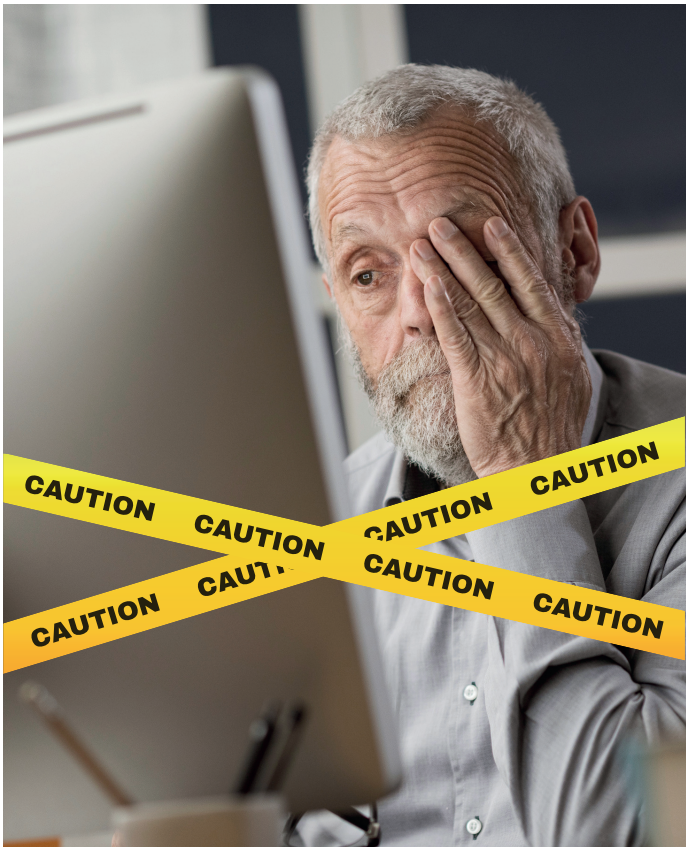
June is officially Senior Scam Month. This targets older adults, however, this could have a drastic impact on how you do business. Learn why they're targeted and discuss safety measures you or a love one can take to avoid dangerous and fraudulent schemes. (*cont.*)

CPD DIRECTOR, ANGELA SELITTO | MARKETING, ROBYN PITT

NEWS & SCAM ALERTS

As a business owner, you understand the importance of safeguarding your assets and investments. However, it's equally crucial to ensure that the seniors in your family are protected from scams targeting their perceived vulnerability, limited technological knowledge, and potentially significant savings or retirement funds. Scammers often prey on older adults, offering bogus investment opportunities with promises of high returns, only to disappear with the seniors' money.

These fraudsters use various tactics to deceive older adults, such as posing as government officials, fake charities, or even as family members in need of financial assistance. It is essential for seniors and their families to be aware of these scams and take steps to protect themselves from falling victim.



Tips for Business Owners to Protect Their Families:

Educate Your Family: Make sure your senior family members are aware of common scams. Discuss the tactics scammers use and emphasize the importance of caution.

Cautious Communication: Encourage seniors to be wary of unsolicited phone calls, emails, or messages asking for personal or financial information.

Identity Verification: Teach them to verify the identity of anyone requesting sensitive information, especially if they claim to be from a government agency or financial institution.

Personal Information Protection: Advise them never to give out personal information, such as Social Security numbers or bank account details, to anyone they do not trust.

Research and Verify: Stress the importance of researching any charity or organization before making a donation, and to be wary of high-pressure tactics to give money quickly.

Stay Informed and Share: Keep up-to-date with the latest scams targeting seniors and share this information with your family. By staying vigilant and informed, seniors can reduce their risk of falling victim to scams and protect their hard-earned savings.

As a business owner, your insight and leadership can extend beyond your business and into your personal life by ensuring your family is well-protected. If you or a loved one suspects that you have been targeted by a scam, report it to the appropriate authorities, such as the Federal Trade Commission. Stay safe and informed.

Job Related Scams are on the Rise in North Carolina

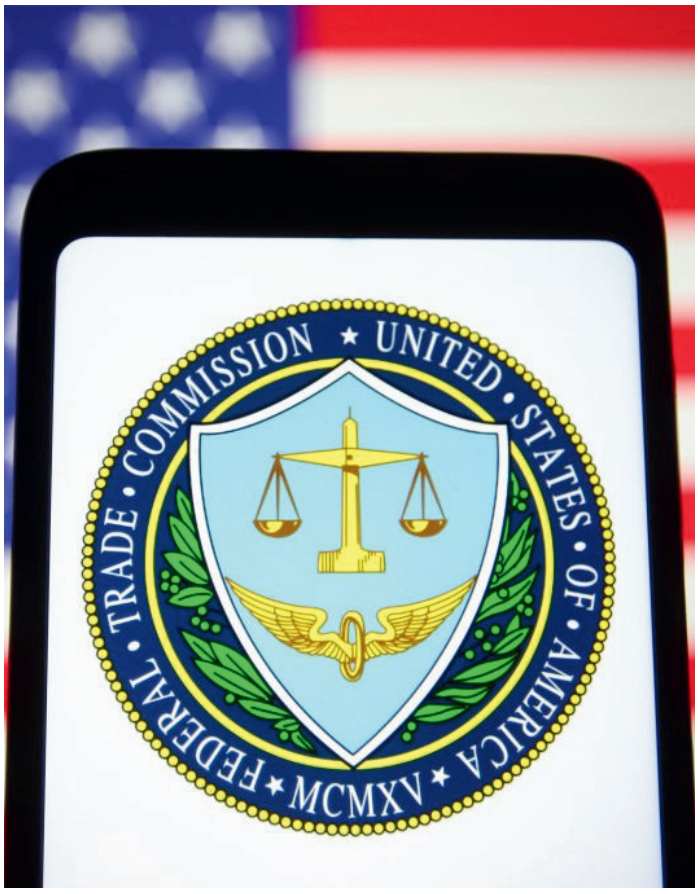
In North Carolina, the state's Department of Justice has highlighted the prevalence of scams that involve impersonating businesses and government officials. These scams often involve fraudulent communications that pressure individuals to act quickly, such as fake job offers or urgent requests for personal information (NCDOJ).

Scammers impersonate legitimate companies or recruiters to collect personal information or money from job seekers. They often ask for upfront fees for job equipment or processing, which legitimate employers would never do (NCDOJ) (Consumer Advice).

Moreover, other common scams include technical support scams, where fraudsters claim to be from well-known tech companies to gain access to personal devices and steal information, and payday loan scams, which target individuals in urgent need of cash by posing as legitimate lenders (www.top10.com).

To protect yourself from these scams, it is crucial to research companies and verify job offers directly through official company websites or known contact numbers. Never provide personal information or payment upfront without thorough verification, and report any suspicious activities to authorities such as the Federal Trade Commission (FTC) (Consumer Advice).

For more detailed information on how to recognize and avoid these scams, you can visit the FTC's Consumer Advice page.



Exposing the Underbelly: Common Scams Targeting Small Businesses

In the vibrant landscape of small businesses, where dreams are nurtured and ventures flourish, there exists a darker side that often goes unnoticed until it strikes. Scams targeting small businesses have become increasingly sophisticated and prevalent, posing significant threats to their financial health and reputation. In this edition, we shed light on some of the most common scams and provide insights on how to safeguard your business.

1. Phishing and Social Engineering:
One of the most pervasive scams affecting small businesses is phishing. Cybercriminals impersonate trusted entities through emails or messages to deceive employees into divulging sensitive information or transferring funds. These attacks prey on human trust and can lead to substantial financial losses if not detected early.

Protective Measures: Educate employees about identifying phishing attempts, implement two-factor authentication, and regularly update security protocols to mitigate risks.

2. Fake Invoices and Billing Scams:
Scammers send invoices for services never rendered or products never ordered, hoping the recipient will pay without verifying the legitimacy of the bill. This tactic exploits busy schedules and trust in established vendors.

Protective Measures: Implement rigorous invoice verification processes, maintain a list of authorized vendors, and conduct regular audits of financial transactions to detect anomalies.

3. Tech Support and Equipment Scams:
Small businesses are targeted with fake tech support calls or ads offering discounted equipment or services. These scams can result in paying for unnecessary repairs, overpriced equipment, or even
installation of malware on company systems.
Protective Measures: Train employees to recognize tech support scams, verify the credentials of service providers, and avoid making rushed decisions under pressure.

4. Charity and Donation Scams:
Scammers exploit businesses' philanthropic efforts by soliciting donations for fake charities or causes. They use emotional appeals or false affiliations to deceive businesses into contributing funds that never reach intended beneficiaries.

Protective Measures: Conduct thorough research on charities before donating, verify their nonprofit status, and establish a clear donation policy within your business.

Conclusion:
As guardians of our businesses, vigilance, and education are our best defenses against these nefarious schemes. By fostering a culture of awareness and implementing robust security measures, small businesses can minimize their vulnerability to scams and focus on what truly matters — growth, innovation, and serving their customers.

Stay informed, stay vigilant, and together, let's safeguard our small business community against the pitfalls of deception.

OVER 100 BUSINESSES

HAVE COMMITTED TO PUTTING CONSUMER'S FIRST.

TELL US YOUR STORY

You work hard to be consumer-centric,
we work hard to send consumers your way.

1. Have your photo taken
2. Tell us how you put consumers first
3. Be promoted online

SCAN TO ACCESS THE FULL DIRECTORY OF TRUSTED BUSINESSES.

CONTACT ASELITTO@FAYBIZ.COM TO SCHEDULE A TIME TODAY.

Consumer Protection Division

CONSUMER PROTECTION CERTIFIED A Division of Faybiz.com

BUSINESSES YOU CAN TRUST