SCAMS

AFFECTING SMALL BUSINESSES

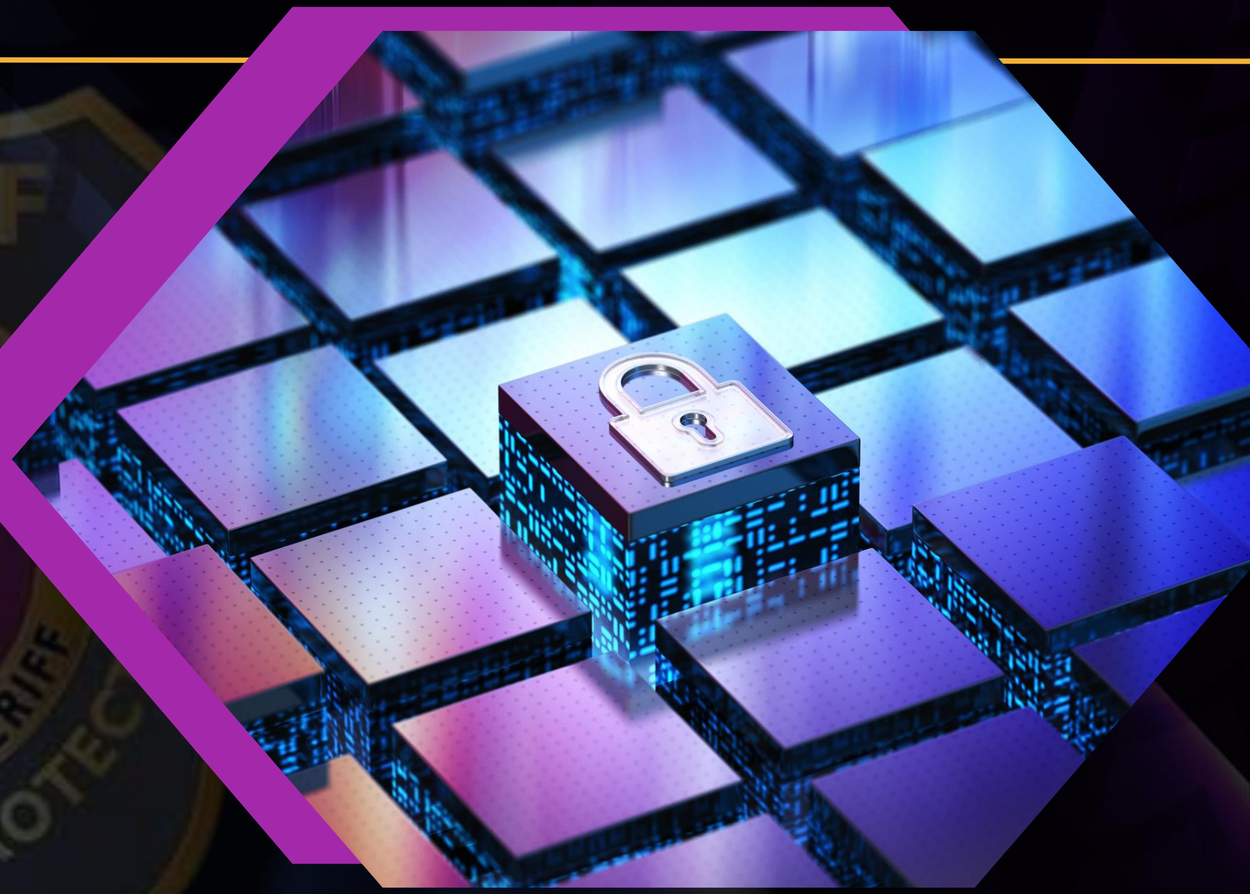
Queen Anne's County
Chamber of Commerce
WHERE SHORE BUSINESS BEGINS

PROTECTING YOUR BUSINESS FROM FRAUD AND DECEPTION

SHERIFF GARY HOFMANN
QUEEN ANNE'S COUNTY
OFFICE OF THE SHERIFF
WWW.QUEENANNESSHERIFF.COM

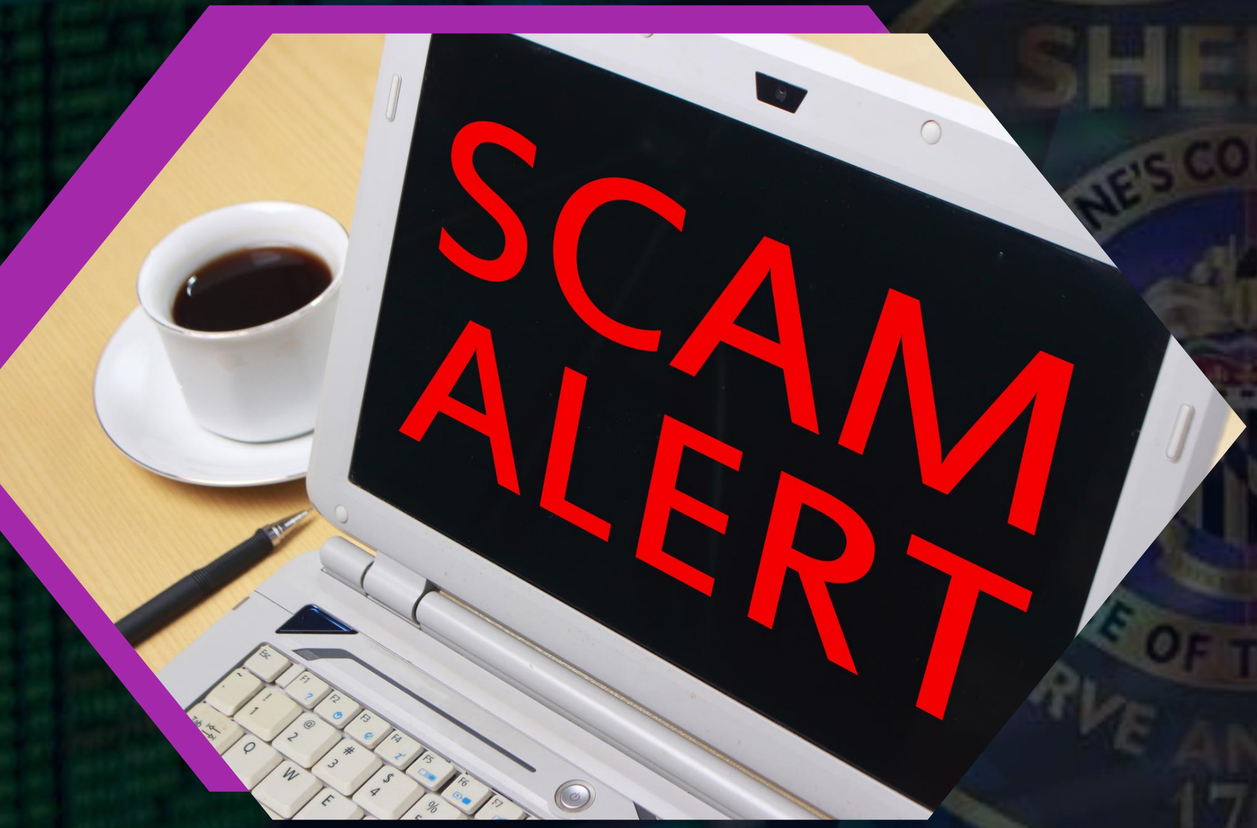
WHY SCAMS TARGET LOCAL BUSINESSES

- **Fewer IT Resources:** Less cybersecurity in place.
- **Limited Training:** Employees may not recognize scams.
- **Trusting Relationships:** Easy to exploit with impersonation.
- **Time Pressure:** Owners often too busy to verify.



Scammers often see small, local businesses as ‘low-hanging fruit’ – busy environments with fewer safeguards than larger corporations.

FAKE INVOICES & VENDOR SCAMS



- Invoice looks real but is fake.
- May use known vendor names.
- Fraudsters send fake invoices for products or services that were never provided. Small businesses may pay these invoices without verifying their legitimacy, resulting in financial loss. Like Delmarva Power having gift cards sent to prevent electric shut off.

PHISHING & EMAIL SPOOFING

- Pretend to be a vendor or a client.
- Ask for wire transfers or account information.
- Use fake email addresses and urgency.
- Fake emails ask for info or payments. Cybercriminals use phishing emails or calls to trick employees into revealing sensitive information, such as login credentials or financial information. This can lead to unauthorized access to business accounts and financial loss.

BUSINESS EMAIL COMPROMISE

Scammers impersonate company executives or trusted partners through email to request wire transfers or sensitive information. These scams can result in significant financial losses.

FAKE JOB POSTINGS & EMPLOYMENT SCAMS

Scammers create fake job listings to collect personal information from applicants or charge fees for “background checks” or training materials that are never provided.

TECH SUPPORT & IT SCAMS

Fraudsters pose as tech support representatives claiming to fix non-existent issues with the business's computer systems. They may demand payment for unnecessary services or install malware.

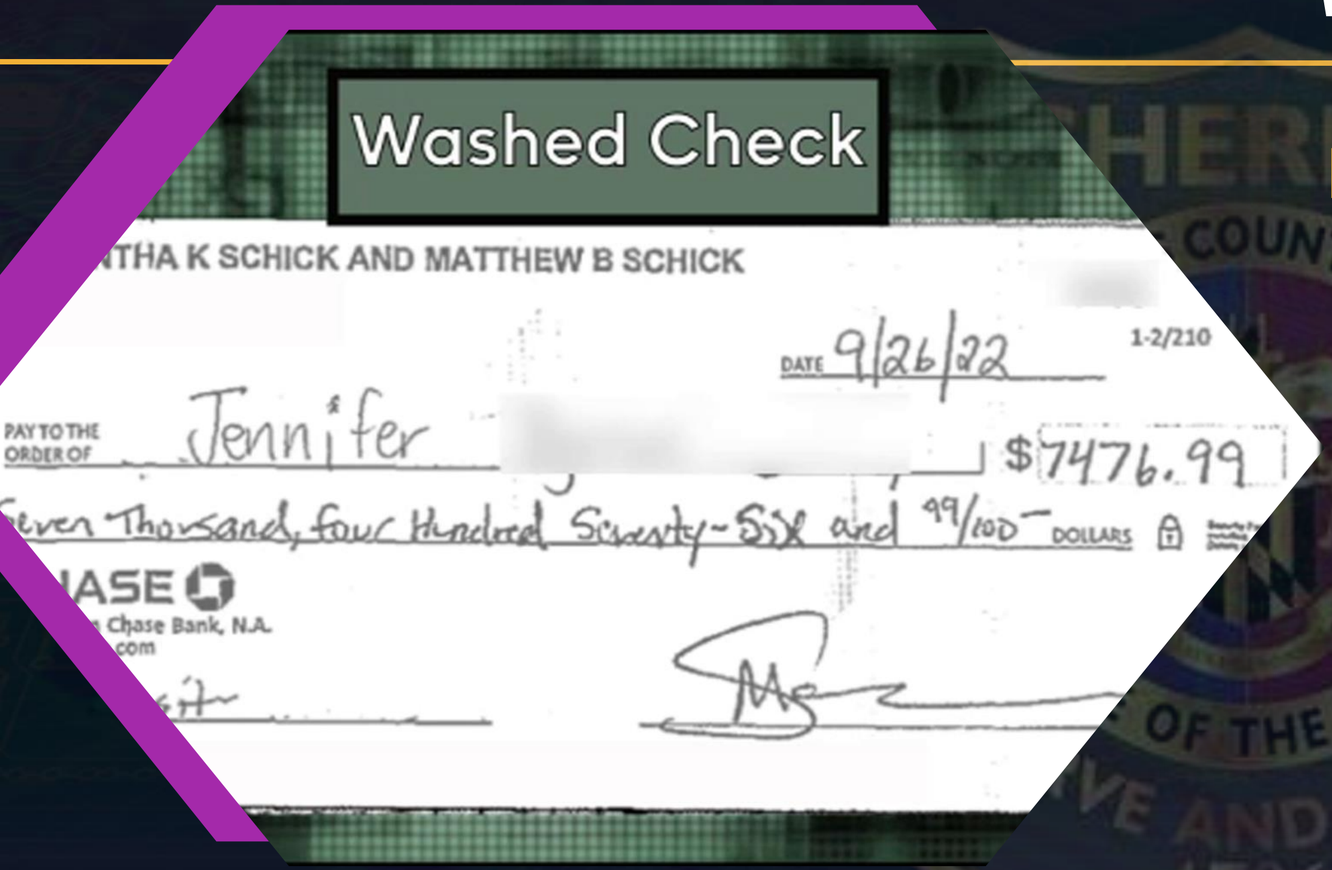
CREDIT CARD & PAYMENT PROCESSING SCAMS

Scammers may offer fake credit card processing services, or steal credit card information during transactions, leading to financial losses.

SHIPPING SCAMS

Scammers trick businesses into shipping goods to fake addresses or individuals, often using stolen credit cards to pay for the items. Similar to Meat Locker, Friel’s, Centreville Lumber, etc.

CHECK WASHING



HOW THE SCAM WORKS

- **Mail Theft** - Scammers steal checks from businesses and mailboxes.
- **Chemical Washing** - Chemicals used to remove ink.
- **Rewriting** - Rewrite with own payee name and new dollar amount.
- **Cashing/Depositing** - Altered checks deposited by variety of methods.

CHECK WASHING

HOW BUSINESSES CAN PROTECT THEMSELVES

- **Use Secure Payment Methods** - Opt for electronic payments whenever possible.
- **Monitor Accounts Regularly** - Set up alerts for check clearances and large withdrawals, monitory statements.
- **Use Security Pens** - Pens with specialized ink.
- **Internal Controls** - Implement measures like two signatures on checks.
- **Shred Old Documents**
- **Report Suspicious Activity**

SKIMMERS

Skimming is a form of fraud where criminals install devices, often disguised as card readers, capture data from the magnetic stripe of cards inserted into the readers. Hidden cameras or keypad overlays can be used to records PINs. This stolen information is then used to create fake cards or make unauthorized withdrawals and purchases.

SKIMMERS

Common Locations:

- Bank ATMs
- Gas Stations
- Convenience Stores

TAX SCAMS

Scammers impersonate tax authorities to threaten small businesses with legal action unless they pay a supposed tax debt. This can lead to fear-based payments without verification.

OVERPAYMENT SCAMS

- Sends check for more than owed.
- Asks for refund of difference.
- Original check later bounces.

RANSOMEWARE ATTACKS

Cybercriminals encrypt business data and demand a ransom for decryption. This can disrupt operations and lead to substantial financial losses.

PROTECTING YOUR BUSINESS

- **Train Staff:** Awareness is key.
- **Verify Requests:** Confirm before paying.
- **Update Systems:** Use antivirus and patches.
- **Shred Documents:** Avoid dumpster fraud.
- **Use Multi-Factorial Authentication:** Extra login security.
- **Establish a law enforcement partnership.**

IF YOU SUSPECT A SCAM

- DO NOT REPLY OR PAY.
- REPORT IT TO LAW ENFORCEMENT OR THE FEDERAL TRADE COMMISSION.
- ALERT YOUR BANK.
- SHARE INFORMATION WITH OTHER BUSINESSES.

RESOURCES

- **FTC.GOV:** Scam alerts and reporting.
- **SBS.GOV:** Business security tips.
- **BBB.ORG:** Business scam tracker.
- **Local Chamber of Commerce:** Peer Support!

FINAL THOUGHTS

- Scammers are persistent and creative.
- Stay alert and informed.
- Let’s protect our local business community.

PHONE APP

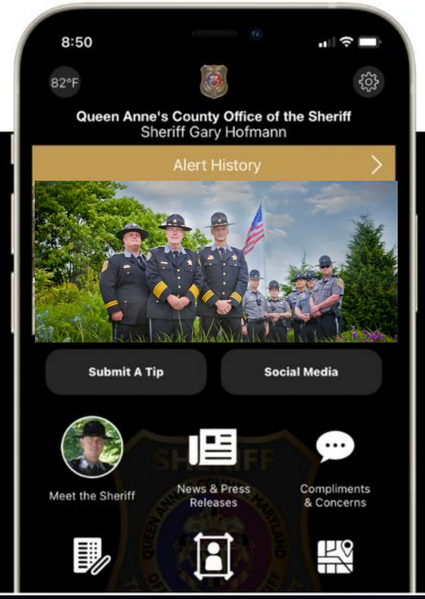
DOWNLOAD OUR APP TO STAY UP TO DATE

Queen Anne's County
Office of the Sheriff

Download our **FREE** mobile app today!

GET IT ON Google Play

Download on the App Store



Thank You!

Sheriff Gary Hofmann

Queen Anne's County

OFFICE OF THE SHERIFF

505 Railroad Avenue

Centreville, MD 21617

410-758-0770