Randolph COMMUNICATIONS

MAY/JUNE 2023

Local Provider.
Endless Possibilities.

RANDOLPH
CONNECTION

THE LATEST SCAMS YOU NEED TO BE AWARE OF IN 2023

While scammers goals remain the same year in and year out, their strategies constantly change with the times. As in previous years, many of the latest scams in 2023 are twists on existing scams, and the measures that have protected you for years can still apply. However, watch out for a few new types of attacks.

1. Student Loan Forgiveness Scams

Student loan forgiveness scammers may contact you via phone or create phony application sites aimed at stealing your Social Security number or your bank account information.

2. Phone Scams

Scammers may try to get in touch with you by phone, and some phone scams rely on smartphones' capabilities to access the internet and install malware.

- Robocalls: They may offer everything from auto warranties to vacations, or issue a threat to try and get your attention. Some robocalls can even respond to your questions.
- Texts: Often, these smishing attempts include a link to a scammer's website or app.
- Impersonators: They often use scare tactics related to your Social Security number, criminal record or account before asking for your personal, account or credit card information.
- Apps: Scammers may try to get you to install a malicious app to steal your information. Or, they might create a nearly identical copy of an existing app and then make money from in-app purchases.
- QR codes: Scammers place their QR codes in inconspicuous spots, and scanning the code could prompt you to make a small purchase or enter your credentials on a look-alike website.

Also beware of two relatively new types of tools and tactics that scammers are using in 2023:

- SIM Swapping: This happens when a thief steals your number and assigns it to a new SIM card in a phone they control.

(Continues on next page)

It's the same process you go through when you get a new phone and the mobile carrier gives you a new SIM card. The scammer uses your SIM card to steal your information to log in to your accounts and either enter a verification code or reset the account password using the code or link sent to the phone.

You might be able to contact your mobile phone operator and add extra security or temporarily freeze number porting to help protect yourself from SIM swapping. Also, see if your accounts let you use a non-SMS multifactor authentication option, in which you provide two pieces of proof to verify your identity.

⚠ One-Time Password (OTP) Bots: An alternative to SIM swapping, some scammers are using so-called OTP bots to trick people into sharing the authentication codes that are sent to them via text or email, or that they have to look up in an authentication app or device.

The bots may initiate a robocall or send you a text imitating a legitimate company. For example, the robocall may look and sound like it's coming from a bank. The voice asks you to authorize a charge and tells you to input the code you're texted if it's not one you made. In reality, the bot is attempting to log in to your account, which triggers the system to send you the code. If you share the code, the scammer can then log in to your account.

3. Zelle Scams

Scammers are turning to Zelle, the peer-to-peer payment app, as a means to steal people's money. The scammer will email, text or call you pretending to work for your bank or credit union's fraud department. They'll claim that a thief was trying to steal your money through Zelle, and that they have to walk you through "fixing" the issue. Then, they may instruct you to send the money to yourself, but the money will actually go to their account.

4. Cryptocurrency Scams

As cryptocurrencies continue to buzz, people may fear missing out on investment opportunities. The scams can take different forms but often involve fake prizes, contests, giveaways or early investment opportunities. The scammers may impersonate celebrities or popular cryptocurrency websites to lure victims into sending them money, sharing login information or "investing" in a project. Crypto exchange accounts have also been the target of OTP bots because you might not be able to get your crypto back if the scammer drains your account.

5. Romance Scams

While romance scams aren't new, their popularity continues to rise. According to the Federal Trade Commission (FTC), people lost $547 million to romance scams in 2021, up 80% compared to 2020 and six times higher than in 2017.

Scammers often steal someone's identity or create fake profiles on dating and social media apps to meet victims. There's no surefire method to detect a fake, although scammers may use stock photos and make excuses for why they can't meet in person.

After gaining your trust, they may ask you to buy them something or send them money. Recently, some scammers have posed as investors and shared false investment tips with their victims, which could lead you to invest in a fake opportunity. Or, the person may "mistakenly" send you money and ask you to send it back or forward it to someone else. If your bank later determines that their payment was fraudulent, the sum of the payment will be subtracted from your account.

Romance scams can target anyone, and some scammers seek to form platonic rather than romantic relationships.

6. Online Purchase Scams

Online purchase scams continued to be the riskiest type of scam in 2022, according to the Better Business Bureau (BBB) 2022 Online Scams Report. The basic premise of this type of scam is that you purchase a product or service that's never delivered. The BBB found that people most commonly reported being victims after trying to buy a puppy online.

Scammers often sell goods on marketplace websites or social media, although some set up fake e-commerce stores. Always look for red flags such as too-good-to-be-true prices, lack of details or high-pressure sales tactics. Scammers may also use triangulation fraud to take money from you when you buy something online, only to purchase the item you want with someone else's stolen credit card. They'll send you the item, and you may never know that they'd used a stolen credit card and pocketed your money.

Paying with your credit card can help you limit potential losses, as you can initiate a charge back if you don't receive a product or service.

Continue Monitoring Your Identity: Be skeptical. Enable multifactor authentication. Research companies before you make a purchase or donation. Be careful with your phone. Don't refund or forward overpayments. Look for suspicious payment requirements. Following basic safety strategies and reviewing the latest scam alerts can help you stay safe.

2023 Liberty Large Business of the Year Award

"We were honored to be awarded the 2023 Liberty Large Business of the Year Award at the recent Liberty Chamber of Commerce Annual Banquet", stated Kim Garner, CEO & General Manager for Randolph Communications. "Randolph Communications is proud to serve Liberty with advanced communication and information technology services; and, we are privileged to support the many activities and events the community hosts each year for its citizens and visitors. Thank you for this distinguished award."

RTMC's 65th ANNUAL MEETING
August 12, 2023

This year's annual meeting will be a business meeting only held outside at our Distribution Center, **6463 Us Hwy 220 South Alt. Asheboro, NC 27205**

Registration will begin at 8:00 am with the business meeting beginning promptly at 9:00 am.

Attendees must be a member or member's spouse to register. Children, grandchildren, other family members or friends cannot register for a member. The meeting agenda includes the election of Directors, a process governed by Article IV, "Board Members," Section 4.5, "Nominations," of the RTMC By-Laws.

It shall be the duty of the Board to appoint, not more than ninety (90) days before the date of a meeting of the members at which Directors are to be elected, a committee on nominations consisting of not less than seven (7) nor more than eleven (11) members who shall be selected from the seven (7) districts so as to ensure equitable representation. At least one (1) member of the committee shall be selected from each district where a Director is to be elected. No member of the Board, close relative of a Director or employee may serve on such committee. The committee, keeping in mind the principle of equitable representation, shall prepare and post at the principal office of the Co-operative at least twenty (20) days before the meeting, a list of nominations for Directors which shall include as many nominees for each Board position as the committee deems desirable;

(b) The Secretary shall be responsible for mailing with a Notice of the Meeting, or separately, but at least ten (10) days before the date of the meeting, a statement of the number of Directors to be elected and the names and addresses of the candidates nominated by the committee on nominations;

(c) Any fifty (50) or more members acting together may make other nominations by petition, and the Secretary shall post such nominations at the same place where the list of nominations made by the committee is posted. Nominations may be made by petition received no more than (90) days and no less than (60) days before the meeting and shall be included on the official ballot. Such ballot shall arrange the names of the candidates by district and shall also designate the candidates nominated by the committee and those nominated by petition. No member may nominate more than one candidate by petition, the seat for which the nomination is made must be specified, and the person so nominated must be in all respects eligible for service on the Board as set out in these Bylaws; and

(d) All Directors must be nominated or re-nominated by the committee on nominations or by petition.

Be sure to watch for more information in early July for information on how to claim your $15 bill credit by completing your proxy if unable to attend. You do not need to be present for the bill credit registration gift.

DON'T MISS OUT ON THE OPPORTUNITY TO SHOWCASE YOUR BUSINESS IN THE 2024 RANDOLPH COMMUNICATIONS DIRECTORY.

Data Publishing is our new directory publisher for the 2024 Directory. They are the only authorized Yellow Pages sales agent for Randolph Communications and one of their representatives will be contacting existing advertisers soon.

If you would like to find out more about how you can help expand your customer base and grow your business just by having your business included in the 2024 Randolph Communications Directory, please call 336-879-7960.

RANDOLPH SECURITY

Don’t wait until it’s too late…

Call **Randolph Security** today!

336-879-5684

www.rtmc.net/security

PAY ONLINE

www.rtmc.net/payonline

PAY BY PHONE

855-382-9920

DATES TO REMEMBER

May 14 - Mother’s Day

May 29 - Memorial Day
(All Business Offices Closed)

June 18 - Father’s Day

PRSRT STD
U.S. POSTAGE
PAID
PERMIT #433
58501

Randolph Telephone Membership Corp. was established in 1954 as a member-owned cooperative now serving eight exchanges in seven different counties. Randolph Telephone provides complete communication services such as local telephone access, business telephone systems, high-speed internet, security, camera surveillance, computer services, web hosting and design and wireless services through its affiliate Randolph Communications.

www.rtmc.net

Liberty
211 West Swannanoa Ave
Liberty, NC 27298
Monday-Friday
8:30am-5:00pm
Closed for lunch from 1:30-2:00pm

Headquarters
317 East Dixie Drive
Asheboro, NC 27203
Monday-Friday
Office Hours: 8:00am to 5:00pm
Drive Thru Hours: 8:00am to 5:30pm

Randolph COMMUNICATIONS

Phone: (336) 879-5684
(336) 622-7900
Fax: (336) 879-2100
Tech Support: (336) 879-5681