Bottom Line Inc. Magazine

■ **Fake job-offer scams** are being used to steal applicants' identities. Scammers post fake job ads on social media or at job-hunting sites, using legitimate groups' names and logos. The thieves interview applicants by phone or online—and get personal information, including bank-account and Social Security numbers, which are used for identity theft. Some scammers send victims a check, supposedly for office supplies or training, with instructions to cash the check and send some part of it back—the check turns out to be fake. *Self-defense:* Do not give out personal or financial information by phone or e-mail…do not agree to wire money, buy gift cards or accept a portion of a check from a supposed employer… beware of job postings offering high pay for simple tasks or a job offer received after only a simple interview—or without one.

Ben Wiseman, director, Office of Consumer Protection in the attorney general's office, Washington, DC, quoted at WTOP.com, a radio station in Washington, DC.

Beware

● **Characteristics that invite fraud and how to change them:** *Respecting authority without question* leads people to believe scammers who call and claim to be government agents. *Thinking you cannot be scammed* can make you more vulnerable to some of the highly sophisticated scams perpetrated by thieves. *Being friendly on social media* invites scammers to pose as friends—limit contacts to real friends and family. *Being in crisis,* because of a recent death or health emergency, increases vulnerability—be especially careful about giving out personal information during times of high stress.

Study by AARP Fraud Watch Network, reported in *AARP Bulletin.*

University Student Email and Voice Mail Scams

University of Arizona students have been targeted by two scams via email and phone related to student employment opportunities and Social Security benefits. *These are malicious scams and not valid communications.*

Student Employment Email Scam

Recent emails from imposters are offering students employment, and providing an initial paper check upon an agreement. Once the student deposits the check, the student is directed to purchase gift cards and send the pertinent information to the 'employer'. Unfortunately, the checks are not valid, and the cost of the gift cards is then incurred by the student.

Social Security Voicemail Scam

Throughout October, UAPD has been contacted by dozens of University students being targeted by malicious callers claiming their social security number was "suspended." The phone number appears to

be either UAPD or a valid university phone number, however it is a "spoofed" number masked as a real number.

Job Opportunity Scam

Since August, University of Arizona students have been targeted by a series of job/internship opportunity scams. They follow a pattern meant to defraud you out of thousands of dollars before you even realize you are being scammed. Once offered the 'job,' you are asked to cash a check in your account to make a withdrawal. Ultimately, that check will bounce and you will be responsible for the insufficient funds drawn from your account (which will have been spent, more likely than not, on gift cards). Many students have already fallen victim to these scams. Please take the following precautions when responding to opportunities for jobs or internships received via email.

TEP Phone Scam https://www.tep.com/news/phone-scam/

Year-round, TEP customers report suspicious phone calls, text messages, letters and even visits from scammers who impersonate TEP employees while using high-pressure tactics.

The Information Security Office wants to make you aware of these scams and to give you the following guidance:

- Social Security Administration(SSA) *does not make phone calls* and will never call to threaten your benefits. Hang up immediately. If you are concerned, the SSA can be reached at 1 (800) 772-1213 or https://www.ssa.gov/
- Verify the senders' email address. Hover over the "from" email address to identify the actual recipient.
- Do not click on Never respond to any suspicious email. Don't click on links or open unexpected attachments.
- Don't believe everything you read. Don't reply to a job offer for which you didn't apply; confirm it by contacting the company or organization.
- Check the links of websites you visit. "Google" the site to ensure the link is correct.
- Never provide personal information, personal or financial via email, text, or over the phone. links and do not open attachments if you do not know the sender.

If you have any other questions or concerns or want to report an incident, please contact the Information Security Office at security@email.arizona.edu or call 24/7 at 520-626-8324 (tech)

Please forward phishes you receive to phish@arizona.edu

If you are ever unsure if an email is valid, you can always reach out to security@arizona.edu

University Email and Phone Scams https://uaatwork.arizona.edu/uannounce/university-email-and-phone-scams

DON'T GET FOOLED

Beware Student-Loan Scams

Mark Kantrowitz
SavingForCollege.com

The Federal Trade Commission (FTC) recently reached a settlement with a pair of companies accused of scamming victims out of more than $20 million by falsely promising to get their student loans reduced or forgiven. Those companies are far from the only ones suspected of operating student-loan scams.

How these scams work: Victims read online ads (or receive phone calls or e-mails) promising access to programs that can reduce or eliminate student loan payments. The scammers might imply they're affiliated with the government. In reality, these scammers usually do nothing more than fill out a simple online form for a US government repayment plan or loan-forgiveness program. Even though borrowers can easily complete this form for free on their own at the US Department of Education website StudentLoans.gov, these companies charge hundreds or thousands of dollars.

Some scammers then instruct victims to make future loan payments to their companies rather than directly to lenders and claim that these payments will be used to pay down the loans. But they pocket some or all of the payments and even might allow the actual loan to go into default. Victims often don't realize this has happened until months or years later, because scammers obtain victims' Federal Student Aid ID (FSA ID) user names and passwords, which lets them alter the contact information on victims' loans.

What to do: Ignore calls, e-mails, online ads and websites promoting help with student loans, and instead visit StudentLoans.gov and click the "Repayment & Consolidation" tab. The only application that's at all tricky is the one for Public Service Loan Forgiveness. But rather than pay lofty fees for help, consult this free checklist—SavingForCollege.com/article/checklist-for-public-service-loan-forgiveness.

Never trust anyone who...

- *Requests payment in advance for help with student loans.* It's illegal to ask for advance payment for debt relief.
- *Promises to get your student loans forgiven.* Legitimate loan-forgiveness programs have very low approval rates.
- *Requests your Federal Student Aid ID (FSA ID) username and password.* Someone who gains access to this data could take out new loans using your name.
- *Mentions the "Obama Student Loan Forgiveness" program*—no such program exists.

Bottom Line Personal interviewed Mark Kantrowitz, author of *How to Appeal for More College Financial Aid* and publisher of SavingForCollege.com.

How to...

Be Safer Online

Steven J.J. Weisman, Esq. Scamicide.com

It seems like there's a new threat lurking on the Internet every day. But there's a relatively easy way to stay safe by using what's called a virtual private network (VPN). Here's what you need to know to get started...

■ **VPNs provide security while keeping users anonymous.** You can download and install VPN software on your phone, tablet or computer just like any other app. Once installed and activated, most VPNs allow users to connect to the service on multiple devices with a single account. The software encrypts the data you send and routes it through secure connections, or "tunnels," to the VPN provider's servers and then to the site you're trying to reach.

Since VPNs channel traffic through tunnels that require authentication from anyone trying to access them, they make the data you send and receive much harder for anyone else to see or steal. This is particularly useful when using public Wi-Fi—a common target of cybercriminals. But there's a second benefit as well. VPNs also provide online anonymity by hiding information about your IP address and making it appear that your data originated not from your computer but from the location of the VPN's servers. Using a VPN can slow down your Internet speed a little, but this depends on a lot of factors such as the distance to the servers you're accessing and the speed of your own home Internet service.

■ **With VPNs, you usually get what you pay for.** There are hundreds of VPN services to choose from, most of which cost between $3 and $12 a month. Many offer free versions, but consider the risks before playing it cheap when it comes to online security and anonymity. Free VPNs often either limit the amount of data you can send or limit the data transfer speed. Most free VPN services collect your information and use that data to target you with ads or even sell your information to third parties. More troubling is that criminals have been known to set up free VPNs to steal information from unsuspecting customers looking for security without the expense.

■ **Keep your VPN up to date.** Even VPNs can be hacked. As with all software, there may be bugs and glitches, so it is important to download all security updates offered by your VPN provider as soon as they are available.

Top VPNs: Not all VPNs are created equal. Among the best is NordVPN. At $6.99 to $11.95 per month (depending on plan duration), NordVPN boasts a massive, more-than-5,000-strong global server network, allows up to six simultaneous connections per subscriber and stands by a strong customer privacy policy. The VPN service called Private Internet Access costs $2.91 to $6.95 per month and is among the least expensive VPNs, though it has a feature-rich platform. Finally, consider IPVanish, whose interface is more user-friendly than that of Private Internet Access. It costs $3.74 to $11.99 per month.

Bottom Line Personal interviewed Steven J.J. Weisman, Esq., an attorney and author of *Identity Theft Alert*. Based in Amherst, Massachusetts, he is founder of the scam-information website Scamicide.com.

Photo of hand holding phone with app: Gettyimages/Prykhodov

DON'T GET FOOLED

Google's Mapping Feature—a Magnet for Scams

Zak Doffman Digital Barriers

Many consumers use Google as a digital Yellow Pages to search for nearby plumbers, locksmiths and the like. But it's possible you could get scammed.

A recent *Wall Street Journal* investigation estimated that there are 11 million fake listings on Google's online mapping service, with hundreds of thousands more appearing every month. These listings often are created by unlicensed or underqualified individuals who do shoddy work and/or charge grossly inflated rates.

How the scams work: When you type your search query in a regular Google search, the top results include a Google map with red pushpins indicating the businesses nearest to you. A shady business may flood a geographic area with dozens of fake listings that appear closer to you and more legitimate than they really are...and that show up at the top of your Google search. In some cases, when you call the phone number, it connects to a referral service in another part of the country or overseas. The service is impersonating a local business in order to secure leads and make money selling your inquiries to unvetted third parties in your area.

Google says that last year more than three million listings were removed for violating its verification and usage policies. However, the problem is likely to persist because it's free to list a business and scammers have been able to stay ahead of Google's attempts to improve verification safeguards. To protect yourself...

Be vigilant about "duress verticals." These are types of businesses most prone to scams because consumers tend to need them during emergencies or on short notice. They include car-towing and car-repair services...electricians...furniture movers...locksmiths...personal-injury lawyers...plumbers...and water-damage contractors. If you do pick a business off a Google map, at least search for consumer reviews about it on a moderated site such as Yelp.com.

Watch for telltale signs of an illegitimate Google mapping business. There's no other information in the listing other than the "NAP" (name, address and phone number)—no business hours or links to its website.

Bottom Line Personal interviewed Zak Doffman, CEO of Digital Barriers, a global cybersecurity company, London. DigitalBarriers.com