HACKERS BRIEF

from CyberWyoming

BE WARY OF EMAILS FROM TUT.COM

As we noted last week, there are a number of email scams being sent from tut.com email addresses. Although we have notified the company many times, we see new ones almost every week. There may be legitimate businesses and persons who use that email address, so you may not want to block all the emails but keep an eye out. Some of the recent ones our citizen reporters have sent us have been for fake service notifications and notices that you've won a $500 gift card or Keurig coffee maker. All these scams contain links that you should NOT click. Reported by a Sheridan citizen.

IGNORE EMAILS FROM AUDU

If you receive an email from Audu Bello at a Gmail address with the subject line of "hello" claiming that Audu has reached out a couple of times but hasn't heard back, don't respond. This is a typical ploy to try to see if your email address is active and if you reply, it will open you up to more scams. Just delete. Reported by a Laramie citizen.

MR. PHILLIP SMITH SCAM EMAIL

Although Mr. Smith claims to be a research assistant from a pharmaceutical company in Spain who is looking for a person in the US to help his company with supply chain issues to produce cancer treatments and "other life saving medications" note that this requests comes from a Gmail address and never really mentions the actual company name. The subject line is "Re: Greetings" as if Mr. Smith was replying to an email you sent. Just delete. Reported by a Laramie citizen.

NEW YEAR'S RESOLUTION TO MANAGE DEBT CAN GO VERY WRONG

The New Year is often when people decide they are going to get a handle on their debt, particularly if they overspent over the holidays. Unfortunately, there are a lot of scammers waiting to take advantage of these well-intentioned people. Some of the scammers go so far as to take upfront payment AND tell you to stop making payments to credit cards and other debts. So now you're out the "fee" as well as even deeper in debt. See https://aarp.info/fwndeb for more details and spread the word to your family and friends.

SOCIAL SECURITY ADMINISTRATION (SSA) WARNING – IMPOSTER SCAMS

Crooks are using fake identity evidence aimed at convincing victims they are government employees, including picture and forged official documents. The Department of Justice recently announced it is increasing efforts with their Transnational Elder Fraud Strike Force to try to combat the social security imposter scams. Here's the scams reported so far:

• Crooks usually call victims, but sometimes even show up in person with forged documents. They claim that the individuals Social Security Number has been suspended because of some problem and often claim that the SSA has overpaid the victim and the victim must pay the SSA back immediately.

• Other scammers say that there is a problem with the victim's bank account and they need to move their money to a "safe" account, stealing the victim's money.

• Letters have been spotted saying victims are entitled to a cost of living adjustment (COLA) and to call a toll free number, which is also a scam.

• Finally, the SSA doesn't sell products or services so don't believe it if you receive a call from the "customer service department."

Avoid scams by always checking with the bank or calling the real SSA at 800-772-1213. Never give your social security number over the phone and never pay in untraceable methods like cash, cryptocurrency, gift card, or money-wiring services. If you think you have been scammed tell the SSA at https://secure.ssa.gov/ipff/home. For more information about spotting a SSA imposter scam check out: https://www.ssa.gov/scam/.

MALICIOUS CODE IN MICROSOFT EXCEL

After Microsoft introduced more protection for Microsoft Office from malicious code introduced via add-ins, hackers found a new way to exploit through XLL files in Microsoft Excel. Before the XLL file can be run and infect a system, Microsoft will display a security message warning the user there is no digital signature available. Users must make sure to click "Leave this add-in disabled."

MS-ISAC AND CISA PATCH NOW ALERT

The Multi-State Information Sharing and Analysis Center (MS-ISAC) or the Cybersecurity & Infrastructure Security Agency (CISA) has published a patch now (update your software) alert for Sophos Firewall, Mozilla Firefox browser, Mozilla Firefox Extended Support Release (ESR), Oracle applications and database (the quarterly critical patch is available), Junos OS (the operating system for Juniper network products), Brocade Fabric OS.

Other ways to report a scam:

• Better Business Bureau Scam Tracker: www.bbb.org/scamtracker/us/reportscam

• File a complaint with the Federal Trade Commission at ftc.gov/complaint

• Report your scam to the FBI at https://www.ic3.gov/complaint

• Reported unwanted calls to the Federal Trade Commission's Do Not Call Registration. Online at https://complaints.donotcall.gov/complaint/complaintcheck.aspx or call 1-888-382-1222, option 3

• Office of the Inspector General: https://oig.ssa.gov/

• AARP Fraud Watch Network (any age welcome) Helpline 877-908-3360

GUEST COLUMN |

It's time for your checkup

ANDREW ELLSWORTH |

Recently I received a mailing from my clinic reminding me it is time to schedule my annual preventative care physical. Apparently, doctors need to go to the doctor, too, even when they feel fine.

As a primary care physician, one of my passions is preventative care. Preventative care is focused on catching problems before they even start to cause symptoms, catching issues early when they are easier to treat.

Whether you want to call it your annual physical, your yearly checkup or an annual wellness visit, this appointment gives the time for you and your provider to decide what tests, screenings and interventions may be done to help you become and stay more healthy. One of the broken aspects of our health care system is our focus on problems, playing whack-a-mole, barely getting ahead and spending too much money way too late on problems that could have been cured a lot sooner, a lot cheaper, with a little bit of effort at prevention.

This visit may go in a variety of ways depending on your age and risk factors. If you are over age 45, you should probably consider your options for colon cancer screening. If you are a woman older than age 40, perhaps you should consider breast cancer screening. If you are a man older than age 55, perhaps you should consider prostate cancer screening. Any of these screenings may need to start earlier if you have a family history of cancer. Meanwhile, the visit should probably include a discussion on your mental health, your diet and your exercise routines. Granted, these discussions take time. If you have a list of problems and symptoms you want to discuss, then perhaps you may need a separate visit to address your concerns, apart from the appointment to cover some of these preventative care topics.

Perhaps this visit will help give you a nudge to quit smoking and a chance to catch lung cancer early by scheduling a screening CT scan of your lungs. Perhaps this visit will determine that you have high blood pressure or high cholesterol and interventions could decrease your risk of a heart attack or stroke. Perhaps this visit will catch skin cancer early. Perhaps your provider will identify a medication you do not need anymore, or identify an over-the-counter medication or supplement you should or should not be taking such as vitamin D or aspirin. Are you taking your medications correctly?

The list goes on and on. Pap smears for cervical cancer screening. Reviewing your immunizations and updating a tetanus shot. DEXA scans help determine the strength of your bones and catch osteoporosis, trying to decrease your risk of a fall and a hip fracture.

I suppose I better make that appointment for myself.

ANDREW ELLSWORTH, M.D. is part of The Prairie Doc® team of physicians and currently practices family medicine in Brookings, South Dakota. Follow The Prairie Doc® at www.prairiedoc.org and on Facebook featuring On Call with the Prairie Doc® a medical Q&A show based on science, built on trust for 21 seasons, streaming live on Facebook most Thursdays at 7 p.m. central.

How to safely use payment apps

BY KIMBERLY PALMER
NERDWALLET

As a frequent PayPal user, I wasn't surprised to see a payment request on the app pop up. But when I read it, I knew something was wrong.

In the message, a stranger asked me to send them $699 in order to get a "refund." While I instantly recognized the request as a scam, I still felt vulnerable; I didn't immediately see any obvious way to flag the request as a scam, and with just one click, I could have accidentally sent this stranger a huge chunk of money.

I'm hardly alone in my worry over security when using peer-to-peer payment apps: According to a Pew Research Center survey published in September 2022, about one-third of people who use payment apps or websites say they are "a little or not at all confident that payment apps or sites keep people's personal information safe from hackers or unauthorized users." And an alarming 13% of people who have ever used PayPal, Venmo, Zelle or Cash App say they have made the mistake of sending money to a scam artist.

Fraud prevention experts recommend these strategies to keep your money safe.

ONLY SEND MONEY TO PEOPLE YOU KNOW

Generally, peer-to-peer payment apps are designed to send money between friends — not strangers. If you use them to send money to someone you don't know, then you put yourself at risk for fraud.

"You shouldn't send money unless you've met people in real life and know who you are sending money to. If you do that, and you're careful in terms of what number you are sending money to, these apps can be a convenient, safe and efficient way to move money," said Paul Benda, senior vice president of operational risk and cybersecurity at the American Bankers Association, a trade association for the banking industry.

USE CASH AND CREDIT CARDS IN HIGHER-RISK SITUATIONS

If you need to exchange money for goods or services with someone you don't know, the safest way to do that is through cash or credit cards, said Axton Betz-Hamilton, an assistant professor in the School of Health and Consumer Sciences at South Dakota State University and author of "The Less People Know About Us," a memoir about identity theft.

Credit cards, for example, come with fraud protection attached. "I want that protection, so I don't use these apps," she said.

While stolen cash can be harder to recover, it may be covered by homeowners and renters insurance policies (up to your policy's limit and depending on your policy).

BE WARY OF TEXTS, CALLS OR UNSOLICITED REQUESTS

Frauds are often perpetuated when scam artists send a text, phone call or other kind of message urging you to send money, perhaps claiming you are due a refund or late on a bill.

"Fraudsters continue to get better at what they do," said Joel Williquette, senior vice president of operational risk policy at Independent Community Bankers of America, a trade group for community banks. That includes sending emails that are almost indistinguishable from legitimate banking emails.

A cybercriminal might impersonate the IRS or FBI and ask you to send a peer-to-peer payment immediately to satisfy a debt, but Williquette said legitimate agencies will never contact you by text or call your cell phone with an urgent request for money.

"Typically, they will send you a letter," he said, and they don't ask for payment through apps or gift cards — another red flag.

A fraudulent payment request sent on a peer-to-peer payment app is "usually for a small dollar amount and might even look like it's from a friend," said Eva Velasquez , president and CEO of the Identity Theft Resource Center, a nonprofit organization.

Velasquez urges people to verify requests first by double-checking they are sending money to the correct person, adding that it's easier to fall for scams when you're distracted and multitasking.

UPGRADE YOUR CYBER HYGIENE

Enabling two-factor authentication on financial accounts, adding a pin lock to your phone and using unique passwords that are at least 12 characters long can help keep you safe, Velasquez said.

In addition, she suggests setting your app privacy settings to the most private option to minimize the amount of information about you that's publicly available.

FLAG FRAUD ATTEMPTS

According to PayPal, if you receive a payment request like the one I got, you should cancel the request without paying. Additionally, you can take a screenshot and forward it to phishing@paypal.com. PayPal adds that you should not reply, open links, download attachments or call any phone number included in the request.

If you mistakenly disclosed any financial or personal data to a scam artist, PayPal said you should change your password immediately, alert your bank and report any unauthorized payments to PayPal.

You can also report your fraud to the Federal Trade Commission at reportfraud.ftc.gov, a government website that shares information with law enforcement.

In my case, I followed the recommended step of canceling the payment request and never heard from my scam artist again. With enhanced security steps in place, I plan to continue to take advantage of the convenience of PayPal and other payments apps — and now I know what to do next time I get an unsolicited payment request.