

Exchange Bank

10 Ways to Avoid Fraud

MEMBER FDIC

JANUARY 2017

Inside this issue:

10 Ways to Avoid Fraud	1
"May you live in interesting times"	2
Safeguarding Taxpayer Data	
Event Calendar	3
Day At the Races—Fonner Park, Grand Island	3
Make a Wish Upon a Cloud Concordia, KS	3
Rent a Safe Deposit Box	4

Scam artists in the U.S. and around the world defraud millions of people each year. They use the phone, email, postal mail, and the internet to trick you into sending money or giving out personal information.

Here are 10 things you can do — or not — to stop a scam.

1. Know who you're dealing with. Try to find a seller's physical address (not a P.O. Box) and phone number. With internet phone service and other web-based technologies, it's tough to tell where someone is calling from. Do an online search for the company name and website, and look for reviews. If people report negative experiences, you'll have to decide if the offer is worth the risk. After all, a deal is good only if you get a product that actually works as promised.

2. Know that wiring money is like sending cash. Con artists often insist that people wire money, especially overseas, because it's nearly impossible to reverse the transaction or trace the money. Don't wire money to strangers, to sellers who insist on wire transfers for payment, or to anyone who claims to be a relative or friend in an emergency and wants to keep the request a secret.

3. Read your monthly statements. Scammers steal account information and then

run up charges or commit crimes in your name. Dishonest merchants bill you for monthly "membership fees" and other goods or services without your authorization. If you see charges you don't recognize or didn't okay, contact your bank, card issuer, or other creditor immediately.



4. After a disaster, give only to established charities. In the aftermath of a disaster, give to an established charity, rather than one that has sprung up overnight. Pop-up charities probably don't have the infrastructure to get help to the affected areas or people, and they could be collecting the money to finance illegal activity. For more donating tips, check out consumer.ftc.gov.

5. Talk to your doctor before you buy health products or treatments. Ask about research that supports a product's claims—and possible risks or side effects. In addition, buy prescription drugs only from licensed U.S. pharmacies. Otherwise, you could end up with products that are fake, expired, or mislabeled—in short, products that could be dangerous to your health. Learn more about buying health products online at consumer.ftc.gov.

6. Remember there's no sure thing in investing. If some-

one contacts you with low-risk, high-return investment opportunities, stay away. When you hear pitches that insist you act now, that guarantee big profits, that promise little or no financial risk, or that demand that you send cash immediately, report them at ftc.gov.

7. Don't send money to someone you don't know. Not to an online seller you've never heard of—or an online love interest who asks for money. It's best to do business with sites you know and trust. If you buy items through an online auction, consider using a payment option that provides protection, like a credit card.

8. Don't agree to deposit a check and wire money back. By law, banks have to make funds from deposited checks available within days, but uncovering a fake check can take weeks. You're responsible for the checks you deposit: If a check turns out to be a fake, you're responsible for paying back the bank. No matter how convincing the story, someone who overpays with a check is almost certainly a scam artist.

9. Don't reply to messages asking for personal or financial information. It doesn't matter whether the message comes as an email, a phone call, a text message, or an ad. Don't click on links or call phone numbers included in the message,

either. It's called phishing. The crooks behind these messages are trying to trick you into revealing sensitive information. If you got a message like this and you are concerned about your account status, call the number on your credit or debit card—or your statement—and check on it.

10. Don't pay a foreign lottery. It's illegal to play a foreign lottery. And yet messages that tout your chances of winning a foreign lottery, or messages that claim you've already won, can be tempting. Inevitably, you have to pay "taxes," "fees," or "customs duties" to collect your prize. If you must send money to collect, you haven't won anything. And if you send any money, you will lose it. You won't get any money back, either, regardless of promises or guarantees.



“May you live in interesting times.”

I've noticed that this alleged Chinese curse seems to be popping up with greater frequency lately. And while I'm not sure we've done anything to the Chinese to warrant it, we certainly seem to be living in interesting times.

I took a little closer look at the origins of this “curse” and found that no such Chinese saying has been found to exist. The closest reference is to an ancient and common maxim “Better be a dog in peace than a man in anarchy,” Since the Chinese culture had lived for so many years in relative peace, they were skeptical of turmoil and change. They believed that the worst of men are fondest of change, hoping to benefit themselves. During times of peace and tranquility, bad people had little to gain. As we've pointed out in other articles in this newsletter, lots of bad people are working hard to take illegal advantage of the new technology we have available today.

As we embark on another year and wend our way through these “interesting times”, we hope that you find peace and tranquility in your friends and family, in home and community and in all the people you live and work with. And while interesting things will continue to happen in 2017 and beyond, we will work hard to make sure that your relationship with Exchange Bank is one of the things you can always bank on, along with a friendly smile, a warm hello and a sincere concern with your financial future. Our goal is not to be interesting but to be a sound, stable and reliable place to take care of all your banking needs.

All of us at the Exchange Bank wish you a safe and prosperous New Year and look forward to seeing you in the coming year.
Craig Dewalt
Executive Vice President

Safeguarding Taxpayer Data – Avoid Scams

Tax return preparers should beware of various ruses and schemes used by cybercriminals. These scams allow criminals to gain access to passwords or computer systems which allows them to steal taxpayer data. Many schemes are currently making the rounds. Protect your clients and yourself from these ongoing and increasingly sophisticated efforts to steal data.

How serious is this threat? Here are a few examples of criminal scams and schemes intent on stealing your information from just the past few months:

In April and August of 2016, the IRS sent emergency alerts to tax professionals about criminals using remote access technology to gain control of preparers' computers. The criminals used the preparers' systems to complete client tax returns, file them with the IRS and then direct the refunds to their personal bank accounts. How the criminals gained control of preparers' computers is under investigation. However, the incident shows the value of strong passwords, not only to access computers and each client file but also to password-protected wireless systems.

One successful scheme aimed at payroll professionals could easily have migrated to tax preparers. A criminal created a “spoofing” email to appear as though it came from a company executive. The email requested Form W-2 information for each employee. Because of this scam, tens of thousands of Forms W-2 were sent to identity thieves.

One ruse tries to make tax preparers think a client is emailing with follow-up information from a previous discussion. The included attachment doesn't contain tax information; it contains malware designed to infect computers. The conversational tone of the phishing email tries to trick the preparer into thinking he had an earlier conversation with this client and now the ‘client’ is following up with requested tax information.

Cybercriminals often pose as the IRS and request information that the IRS would never ask for via email or text. One popular scam tries to trick preparers into providing their password information for IRS e-Services accounts. The email to tax preparers asks them to update their e-Services accounts. It either infects the preparers' computers with malware that tracks keystrokes or it sends preparers to a fake e-Services page where they enter password information. If you are in doubt about an e-Services or IRS Quick Alert communication, go directly to the application through IRS.gov. Do not click on any link or attachment from a suspicious email.

Scams aimed at tax preparers evolve each year. Tax professionals must be aware that any email can be a possible ploy from a clever criminal. This is just a sampling of scams. See Publication 4557, Safeguarding Taxpayer Data, for steps to protect your client and protect your business.

2017 CALENDAR DATES TO REMEMBER..

Monday, January 16th—Closed in observance of Dr. Martin Luther King Jr. Day

Tuesday, February 14th— Valentine's Day, Stop by and get a FREE ROSE!

Monday, February 20th— Closed in observance of President's Day

Sunday, March 12th—Daylight Saving Time Begins

Friday, March 17th—St. Patrick's Day

Sunday, March 20th—Spring Begins

Friday, March 24th—Day at the Races, Grand Island

Friday, April 14th—Good Friday

Friday, April 14th—Visit the Easter Bunny at Exchange Bank

Friday, May 12th— Mother's Day, Stop by and get a FREE ROSE!!

Snowbirds—Remember to contact us when you arrive home so we can change your address.

Watch for more upcoming trip information!



**Exchange Bank
Invites
our 55 Club to a
Day at the Races!!**



Where—Fonner Park, Grand Island

When—Friday, March 24, 2017

Time—Club House Doors Open @ 2:00 p.m.

First race starts @ 3:00 p.m. 10 Races

Come join us for a fun-filled day!

Includes concessions and drawings!

RSVP by March 17, 2017

Grand Island—308-382-2900 or 308-384-8000

Gibbon—308-468-5741

Kearney—308-237-7711

Lincoln—402-328-8527



More info coming
soon!!

“MAKE A WISH UPON A CLOUD”

Cloud County, KS (Concordia)

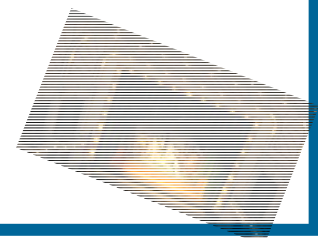
Thursday, May 18, 2017



Come join Exchange Bank to Cloud County Kansas that is, more specifically, Concordia. You'll be amazed at the interesting sights and attractions that are in store for you.

We will visit the National Orphan Train Museum, The Brown Grand Theatre, The Whole Wall Mural, Sisters of St Joseph Convent, Cloud County Historical Museum and the WWII German POW Camp. Also including a delicious lunch at Marla's Joy Tea House.

Mark your calendars and watch for more information in your statements!!



1204 Allen Drive
PO Box 5793
Grand Island, NE 68802
939 South Locust St
Grand Island, NE 68801
14 LaBarre
PO Box 760
Gibbon, NE 68840
3110 2nd Ave
PO Box 397
Kearney, NE 68848
7655 Pioneers Blvd
Lincoln, NE 68506



Shoebox in the Closet?

It is now more important than ever to make sure you have all of your important documents: wills, insurance documents, titles, and personal valuables in a safe place. Most of us use a “shoebox in the closet” method. May we suggest a much safer way? Rent a Safe Deposit Box from Exchange Bank! We have boxes available. They range in size depending on your need. We bill once a year and can have the amount automatically deducted from your account at the bank. Our safe deposit boxes are a safe choice for your important items rather than that shoebox in the closet.

So gather up all your important documents and personal valuables and open a safe deposit box!!

