A publication brought to you by Ihry Insurance Agency, Inc.

# Ihry News

October 2018

Let us know how we are doing by providing a review on Google or Facebook!


Contact Us:

Devils Lake
701.662.5027

Hillsboro
701.636.2540

Hope
800.726.7929

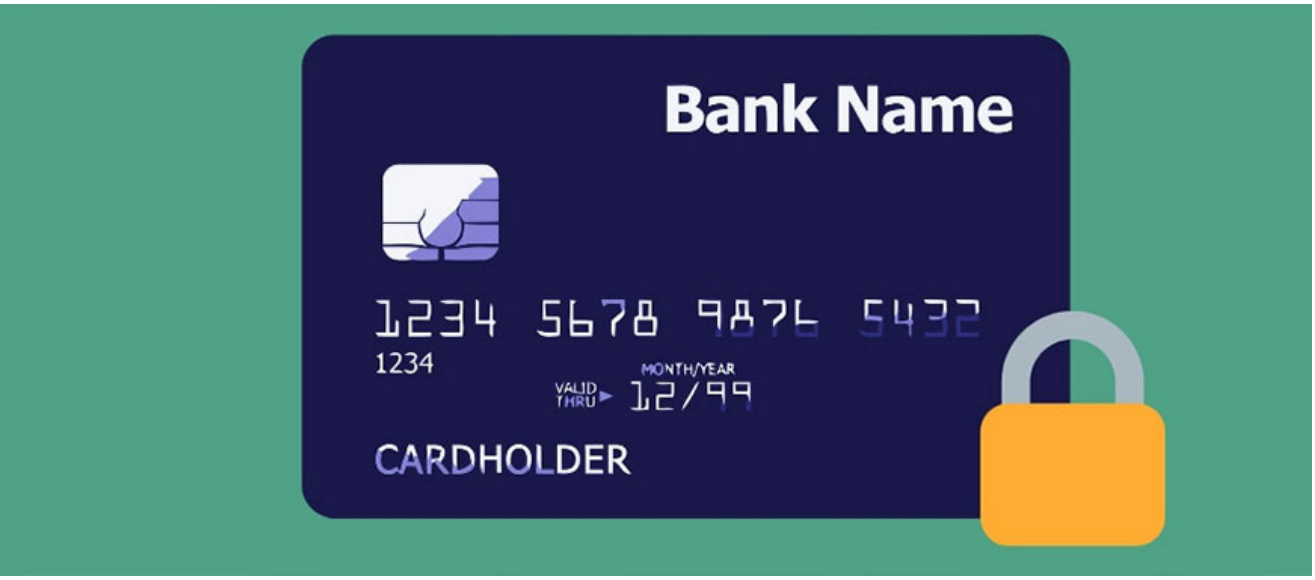
Mahnomen
218.935.5830

McVille
701.322.5553

Towner
701.537.5942

West Fargo
701.492.2228

www.ihryins.com


## Best Ways To Prevent Credit Card Fraud

*Article provided by Ihry Insurance.*

With credit card fraud, identity theft, and data breaches dominating the headlines in recent news, it's hard not to have some concern.

While recent credit card tech, such as EMV chips, promises to make some payments safer, most fraud experts predict credit card fraud will remain a growing problem for years to come.

With the inevitableness of this reality, let's explore some fraud stats and the best ways to prevent credit card fraud.

### What Is Credit Card Fraud?

Credit card fraud is the unauthorized, illegal use of your credit card to either obtain goods without paying for them or obtain funds from your account by way of a cash withdrawal.

Moreover, most card fraud occurs in the United States. The U.S. is responsible for nearly 50% of the world's card fraud, despite only accounting for 25% of total worldwide card volume. The primary reason? The slow adoption of EMV chips and aggressive level of online shopping.

### Most Common Types of Credit Card Fraud:

- Online (card not present) – 45%
- Counterfeit (skimming) – 37%
- Lost/stolen – 14%
- Other – 4%

### Best Ways To Prevent Credit Card Fraud:

While it's important to know what to do when you're a victim of credit card fraud, proactively protecting your sensitive information can prevent you from falling victim in the first place.

### 1. Be Aware of 'Phishing'

Phishing is a scam to trick consumers into revealing personal information. Avoid providing information to any sources you don't fully trust.

### 2. Secure Sites Only

Only provide credit card and personal information on secure websites. Secure sites are denoted with a lock symbol or 'Secure' next to their web address.

### 3. Get The Chip

EMV chip cards are helping to alleviate fraud from device skimmers (stealing card information from credit card swipes.) However, if you see something unusual in the card slot, don't use it.

### 4. Pay With Your Phone

Smartphone-based payment services, such as Apple Pay and Android Pay, use tokenization technology. This tech changes payment information with every transaction, so no definitive information can be obtained.

### 5. Avoid Wi-Fi

When using public Wi-Fi with any device, don't pay bills or make purchases. Public Wi-Fi is extremely vulnerable. Only make purchases on private connections.

### 6. Don't Save CC Info On Sites

While this may be a stretch for most, one of the best ways to protect your CC info is to not store the information on websites. If possible, try to manually enter CC info every transaction.

### 7. Unique Passwords

We all face the woes of forgetting a password. We get it. However, using a unique password for all sites you have stored your CC on is proven practice for protecting yourself. Write your passwords down. It's that simple.

### 8. Travel Belt

When traveling, secure your credit card in a travel belt. While it looks nerdy, we'd rather look nerdy than distraught.

## Ihry Insights

Be safe this harvest!

*Article provided by Curtis Kaufman, Agency Manager*
*Ihry Insurance*

## Farm Bill- Update

### Farm Bill Progress: Perspective From Ranking Member Peterson

October 1, 2018

- House Ag Committee Ranking Member **Collin Peterson** (D., Minn.) **"We've made very good progress this week.** We've had a number of calls. **Right now we're waiting on scores on a couple of things.** And that's kind of what held us up yesterday afternoon, because we don't have these couple of things that were put on the table by Chairman Conaway, I guess it was Tuesday, which get us, in my opinion, in the range of getting this thing done.

- Rep. Peterson reiterated that the nutrition title is not what is holding up progress on the Farm Bill at this point: **"There are other things that have been brought into this that are expensive,"** he said.

- "So I think if we can get this resolved this week and come to an agreement and then we're in the process of drafting it and finalizing it. You know, I think…I don't know exactly…the Senate's in…whether we're going to be in, I think **I've heard there's a possibility that we will be around to be able to pass a bill in October.** So that's the majority's decision, **but I think we can get this done."**

## $12 Billion USDA Farm Aid Package

**Market Facilitation Program**
**Info Update:**

What happens if producer reports under or over the initial self-certification?

- According to Notice MFP-2 issued September 21, 2018, Producers will have one opportunity per MFP commodity to Self-Certify production on the CCC-910, Part C. They can wait to self- certify their production until they sell or gin their crop, or they can self-certify their production prior to selling or ginning. **Once production is self-certified on the CCC-910, Part C, production may not be changed unless loaded in error. EXCEPTION: The production may be reduced by the producer, prior to producer being selected for spot check.**

What are the deadlines on Part C and Part D of the CCC-910?

- The deadline for Part D – Producer Certification is January 15, 2019.
- The deadline for Part C - The production must be self-certified by the producer and loaded in MFP application software by MAY 1, 2019.

I attached a revised CCC-910 to this email. Unfortunately, we can no longer accept the form I shared at the meeting. Please share this information and let me know if you have any questions.

Linsey Bauer
County Executive Director
USDA – Farm Service Agency

## North Dakota: Farmland Values Tested by Rising Interest Rates

Posted on October 1, 2018
By Kelli Anderson, North Dakota State University

- Many commercial row crop farmers across the U.S. have seen their margins squeezed by lower commodity prices and relatively higher production costs, says **Bryon Parman**, North Dakota State University Extension agricultural finance specialist.

- Rents have come down modestly in North Dakota, declining from a high of $69 per acre in 2015 to a statewide average of $65 in 2018.

- Similarly, cropland values in North Dakota mostly have held their value, declining from a high of $2,123 per acre in 2015 to $1,996 per acre in 2018. However, rising interest rates will increase borrowing costs, making operating loans and new land purchases more expensive. Also, as interest rates rise, fixed-income alternative investments become more attractive, likely pushing cropland values down further.

- Interest rates have moved upward steadily since the summer of 2016, while net farm incomes have declined.

- Federal Reserve announced on Sept. 26 that it is raising the federal funds rate 0.25 percent, and economists anticipate that one more rate hike will occur in December 2018.

# PHISH BAIT:

## THREE TIPS TO HELP KEEP YOU FROM A HACKER'S HOOK

*Article provided by Hartford Steam Boiler.*

We all know to watch for suspicious emails. But phishing emails are becoming increasingly more sophisticated, tricking even the savviest among us. Here are three tips to avoid falling for the latest tricks.


### 1. Check the Source

Before you open that email, take a moment to consider the source of the email and whether that person is likely to send you an attachment or link. Did the email come from someone with whom you regularly communicate? Check the email address, screen name, or phone number associated with the message. Hackers often mimic an email address that you would trust with one letter or number off from the original name or domain.

For example, john_smith@company.com looks a lot like john_sm1th@company.co, but the subtle difference dictates whether you are receiving a business email or a malicious fake.

The address may even look exactly like a trusted contact but when you mouse-over the name, you can see that the address is different. A hacked email account can also be used to send malicious content, so be sure to evaluate the content of the message.

### 2. Check the Content

Before you click on a link or download an attachment, take a look at it. Many times, if you copy the link or name of the attachment into a search engine, you can find out whether or not the content is actively being used to spread malicious content (a virus, ransomware, etc.)

Ask yourself whether this is the type of content you usually receive from the sender. Are you expecting an attachment from the sender? Is the attachment or link the only content of the email? If you have the slightest doubt, either delete the message or give the sender a call. The amount of time used to verify the content is relatively short when compared to the time and expense incurred remediating a cyber-attack or data breach.

Hackers often make an urgent request to trick us into clicking on malicious links or files. Any urgent request sent via email should be verified in-person.

### 3. What if I Clicked on the Wrong Thing?

Everyone makes mistakes and you wouldn't be the first person to click on a bad link or download a bad file. Even if nothing happens immediately, there is no guarantee that the threat is gone. Malware can lay dormant for weeks, months, or even years before activation. It may also be transmitting information in the background without your knowledge.


So, take action as soon as you realize you clicked on a bad link or file. Alert your information technology security department right away. If you are a smaller operation, run a virus scan and keep an eye on your financial information.