GRAND MOUND TELECOMMUNICATIONS NEWSLETTER

Quarterly Newsletter Published for our Customers www.gmtel.net September 2014

Latest Hacking Attack: CyborVor – Russian Hackers

On Tuesday, August 5, 2014, it was reported in the U.S. news that a U.S. security firm had discovered a Russian hacking ring had stolen billions of user name and password combinations and more than a half million email addresses.

How do you know if yours was stolen? You don't at this time unless you pay $120 for an annual subscription to find out in the next 60 days if you were affected. This hack is the largest that has been seen in quite some time, even larger than the Target security breach or the Heartbleed virus hacks. At this point, you should assume you were hacked and proceed to change all of your passwords.

Here are a few steps to make your accounts more safe in the event of a future breach:

1. **Change your passwords, especially your bank and any financial passwords.**
   - Use different passwords for different accounts, especially for those that have sensitive information like email or banking.
   - Don't use "dictionary words" and make sure your passwords include a variety of numbers, letters and symbols.
2. **Try a secure password manager.**
   - Connectsafely.org suggests using a program or service like RoboForm, LastPass or PasswordSafe to create strong passwords for each of your sites, but you only have to remember one password to access the program that stores your passwords for you. Another service, Dashline, has also received good recommendations from the New York Times.
3. **Look for unusual charges on all of your financial statements.**
   - Monitor your accounts closely for even the smallest discrepancy. Thieves will often test a financial account with a small charge first to see if it is active AND if anyone is paying attention to that account, and then come the high-dollar charges.
4. **Update the software on your personal computers.**
   - Zombie botnets were probably used to retrieve many of the stolen passwords from personal computers. By downloading the latest operating-system software for your computer, you are ensuring at least a minimum level of protection. Also consider updating your computer's anti-virus security software.
5. **Watch your credit reports.**
   - You are allowed a free credit report from each of the three major U.S. credit bureaus each year. Monitoring your credit report doesn't protect you from identity fraud but it will alert you to any activity that you haven't authorized.
6. **Use a *passphrase* instead of a password.**
   - Enable two-factor authentication on websites that provide it. Avoid using anything that refers to your name, nickname, the name of a family member or pet and any personal numbers like phone numbers, addresses or other information.

Holiday Closing

Grand Mound Coop. Telephone & Grand Mound Communications will be closed on

Monday, September 1st

for Labor Day.

We will reopen on Tuesday, September 2nd at our normal time.

Have a Safe & Enjoyable Labor Day Weekend!

IOWA ONE CALL

Governor Terry Branstad signed into law House File 2408, which amended Chapter 480, Iowa Code, effective July 1. The new laws under Chapter 480 impact both underground facility operators and excavators.

Changes affect white lining prior to excavation, life of a locate ticket, processing time lines and a new ticket status system.

For more information, visit *www.iowaonecall.com*.

NOTICE!

When burning or mowing ditches, be aware of telephone pedestals and equipment. You may not only damage the equipment and cables, but vital emergency services could be cut off to your neighbors or yourself.

SOLAR INTERFERENCE

During the month of October, we will be experiencing solar interference during which degradation or loss of satellite signal will occur on our CATV system.

The paths of the sun on satellite transmissions cause these 10 to 20-minute disruptions.

This will occur between the hours of 2:00-5:00 p.m. for approximately 10 days during October.

NEW DIRECTORY LISTINGS AND UPDATES

-B-

Beam C
2305 Hwy 30 Grand Mound **847-2424**

-D-

DAC ICF
Office 1 907 9th Av DeWitt **659-6620**
House 907 9th Av DeWitt **659-6621**
Office 2 907 9th Av DeWitt **659-6622**
Office 1 915 10th St DeWitt **659-6630**
House 915 10th St DeWitt **659-6631**
Office 2 915 10th St DeWitt **659-6632**
Office 1 916 10th St DeWitt **659-6640**
House 916 10th St DeWitt **659-6641**
Office 2 916 10th St DeWitt **659-6642**
Office 1 1000 10th St DeWitt **659-6650**
House 1000 10th St DeWitt **659-6651**
Office 2 1000 10th St DeWitt **659-6652**

DAC Inc
108 E Industrial St DeWitt.....**659-4100**

-R-

Rothbart J
609 Clinton St Grand Mound **847-3166**

-S-

Soenksen Sarah & Greg N
2608 250th St DeWitt.....**659-9321**

-T-

Touch Of Bliss Salon & Spa
715 5th Av DeWitt.....**659-6166**

IS YOUR COMPUTER INFECTED WITH A VIRUS?

Watch for these symptoms to help you diagnose and treatment.

Frequent Pop-ups?

If you start getting an inordinate number of messages or images while you're online, or worse yet, they appear even when your browser is closed, then it's time to take action. Use a recommended anti-malware software program to scrub your computer and eliminate the virus.

Messages You Didn't Send?

Monitor your "Sent Messages" file and social media posts. If you see a message that didn't come from you, or acquaintances report receiving emails that you didn't send, run your antivirus software and change the password to your account.

Lockdown Warning?

Also called "ransomware," these messages come in a variety of forms. Whatever the demand (which is usually money to unlock or get your computer back), do not respond. It's thievery, plain and simple. Unfortunately, typical antivirus software won't remove this virus. To get rid of it, you'll need a bootable "rescue" CD or USB device.

Crashing, Freezing, or Sluggish Operation?

An infected computer frequently has system crashes, frozen screens and snail's pace operation. If these problems worsen over time, it could just be a configuration issue. But if these glitches appear suddenly, malicious software could be the culprit. Open up your Task Manager to see what your computer is running. If you can't, that's a sure sign of a virus at work. If the computer is operable, run your antivirus program. If it's not, you'll need a bootable virus-removal tool.

Other indications that your computer may have a virus include:

- Unexpected sounds that play randomly
- A message that a program you haven't run has tried to connect to the Internet
- Lots of "system error" messages
- An operating system that won't load when you fire up the computer
- Files or folders that have been deleted or altered
- Programs that start unexpectedly
- A Web browser that behaves oddly or can't close a window

Cybercriminals want access to your information. The longer a virus goes undetected, the longer they have to get what they are after—pilfering passwords, sensitive files and other critical information or using your computer to spread the virus to others. Every computer needs powerful security software running daily to catch malware in hiding, as well as a watchful operator. A virus can wreak havoc on your computer system and compromise your personal information.

Grand Mound Coop. Telephone Assn. and Grand Mound Communications Co.

providing local/long distance telephone services for the Grand Mound/DeWitt areas, PCS Wireless, Voice Mail, Paging Services, data and fax services, fiber optics, CATV, Internet, DSL and Wireless Internet.

(563) 847-3000

705 Clinton Street
P.O. Box 316
Grand Mound, IA 52751

grmd@gmcta.coop

Business Office Hours
Monday to Friday
8 a.m. to 4 p.m.

General Manager
Harry Slaymaker

Office Manager
Terri Bumann

Office Assistant
Dee Dee Banowetz

Combination Technician
Chris Beuthien

Plant Technicians
Nick Wichtoski
Century Schnede