



Notice of Annual General Meeting

The FENN REA will be holding its
Annual General Meeting (AGM) on
Monday, March 16, 2020.

Location: Big Valley Royal Canadian
Legion Hall
Main Street, Big Valley, Alberta

Tel: If you need to contact someone
during the AGM, please call Jolena
Hullmann at 403-742-1449.

Start time: 7:30 pm

Information

As REA members you have a district advantage in that you have the opportunity to attend an Annual General Meeting that is held locally in your REA service area.

The AGM is the perfect opportunity to connect with fellow members and to meet and talk with your Directors.

The AGM is also the occasion where members receive reports on the REA including the President's Annual Report and the financial report. It provides a forum to ask questions and gain more details on your REA's operation.

So mark your calendars and plan to attend – March 16th.

Cybercrime Sets its Sights on Agriculture

Cybercrime is a serious problem for all industries and sectors and as digital transformation sweeps across the agricultural industry, agribusiness is a ripe target.

As farms increasingly adopt Information Technology (IT) they enter the same arena of cyber threat as any other business that uses IT. That risk was noted at the recent FarmTech trade show in Edmonton, where David Masson, a security expert and presenter at the show, spoke to an Edmonton Journal reporter saying, "They

(farmers) have the same IT systems and the same IT security problem as anywhere else in the world."

The reality is that all facets of a farm business, from automated dairy operations, combine GPS, automated water and feed systems to farm financials, are subject to hacking and/or ransom schemes that can disrupt operations.

(cont. on reverse)

For power outages, emergency power troubles and service requests, contact the distribution system operator for FENN REA: **ATCO Electric**
Phone toll-free: 1-800-668-2248

FENN REA
Box 31, Fenn, Alberta T0J 1K0
Phone: c/o Philip Jarmin,
1-403-740-9384
Email: fennrea@gmail.com
www.fennrea.com

Battle River Power Coop
Member Care & Billing
Box 1420, Camrose AB T4V 1X3
Phone toll-free: 1-877-428-3972
Email: brpc@brpower.coop
www.brpower.coop

In January, a Saskatchewan farmer had hundreds of thousands of dollars stolen from the family farm's bank account and he is not alone. In his case the fraud appears to have started with the theft of a SaskTel phone number and email. The family was a victim of a port-out fraud — where a fraudster collects personal information about an individual and then uses that information to open a new account with a new carrier. They then transfer the account over and proceed to steal whatever information is contained therein.

In North America, farmers have reported they were being targeted by several main types of fraud.

- **Business email:** By impersonating a person the farmer may know and trust, the fraudsters try to email farm accounts and convince them to make an urgent payment or to change their account details.
- **Text and phone scams:** Phishing calls and scam texts are easy and cheap for cybercriminals. They attempt to trick targets into divulging personal information or selecting a link which then downloads malware.
- **Phishing emails:** A phishing email is designed to look real but trick you into entering your account details or downloading malicious software. Many of these emails are relatively easy to spot, but more recently attacks have become more credible. Fraudsters can now convincingly mimic the branding and content of well-known organizations which means many people will trust them.

There are some basic security steps you can follow to guard the farm.

- **Secure mobile devices:** Telephones aren't just for talking any more, and farmers' phones probably carry as much data as a desktop computer, so a farm's mobile devices need to be secure. Make sure these devices have the latest in security protections to avoid malware, viruses, or hacking.

- **Secure the farm's Wi-Fi network:** Given the rural nature of most North American farms, computers might be hooked to a satellite internet provider and use modems inside the house. Make sure an encrypted code is in place so only authorized personnel can access it. The same goes for the router if multiple locations on the farm share the same service.
- **Be cautious with emails, browsing and social media:** Delete suspicious emails and do not click on links from unknown sources or pop ups on websites. Be aware that cyber criminals often mine social media for personal information. Use discretion in the information you post publicly.
- **Back up all data:** Properly backing up data will stave off a disaster such as a virus-related crash that erases all records. Read up on what a "cloud system" is, and determine if that or a separate server would be best for your operation.
- **Keep workers informed:** Depending on how your operation is set up, employees and vendors might be sharing your Wi-Fi or bringing laptop computers onto the site. Zip discs and other shared storage devices bring the potential of viruses as well as other security risks.



*Remember --
manage your
digital security
just like regular
equipment
checks and
physical farm
security.*

Regulated Rate Option (RRO)

The RRO rate may increase or decrease from month to month as it is priced on the open market and subject to many factors relating to supply and demand. If you do not have a contract with an electricity retailer, then you receive the default RRO rate.

For January 2020, the RRO is priced at \$0.07101 per kWh, which is reflected on your enclosed bill. For February 2020, the Battle River Power Coop monthly rate as calculated under the RRO regulation and charged to FENN REA members is \$0.08309. The RRO rate is also listed on www.fennrea.com.

Members are free to purchase electricity services from a retailer of their choice. For a list of retailers, visit ucahelps.alberta.ca or call 310-4822 (toll free in Alberta).

Information on FENN REA's Code of Conduct Compliance Plan can be found on our website: www.fennrea.com