

Safety First

How to identify and put a stop to hackers and scammers.

by Megan Silveira, assistant editor

The internet has opened the door to many new business opportunities. Websites allow breeders to showcase their operations to wider audiences, and social apps like Facebook and Instagram allow for direct marketing to new customers. Along with these benefits comes a greater burden to keep yourself safe online.

“Since so many have shifted from using social media just for entertainment or connecting with friends to doing business on these platforms, the stakes are higher now,” says Miranda Reiman, director of digital content and strategy for Angus Media. “There’s a potential to disrupt commerce.”

Reiman and her team understand the threat all too well.

In January, the Angus Media Facebook account was hacked, resulting in the eventual loss of 20,000 followers. The hackers deleted key account information and historical benchmarks. They removed many of the administrative users (or “admins”) from the page within hours of the initial attack, making it even more difficult for Angus employees to address the problem.

“It was all hands on deck that first weekend, and through some key proactive steps, we were able to protect all Angus Media banking

account information, protect others we did business with and warn others about the threat,” Reiman says.

Though the digital team at Angus Media recently launched a fresh Facebook page to continue to provide key data and advertising opportunities to breeders, the threat a hacker poses never truly goes away.

Business pages are a common target, and hackers have a variety of strategies to encourage a response from the real business owner.

“Hackers have really gotten more sophisticated in recent years, so that it used to be almost laughable to think you’d fall for a scam, they’re much more believable today,” Reiman says. “It really can happen to anybody.”

Thomas Medsker, director of information systems for the American Angus Association, encourages producers to be skeptical when they receive new and unfamiliar messages.

“The best advice I can give is to question everything,” he says. “If you aren’t sure about something or it seems wrong, don’t proceed.”

Safety starts from the moment you open a laptop. Medsker says he recommends producers **do not keep passwords in a saved list**. While he admits trying to remember every

password can be a challenge, it provides an extra level of protection.

“A funny but valid way of thinking about passwords is to treat them like underwear,” he explains. “Change them often, don’t leave them laying around and don’t share them with anyone.”

When creating login credentials, **make passwords as strong as possible**. This means combining upper- and lowercase characters with symbols and numbers. Reiman also recommends turning on **multifactor authentication** when applicable. It’s an added safety measure that requires a code be submitted when logging in from a new device.

Beyond logging on safely, Medsker says **there’s value in using a reputable antivirus software**. Whether loyalties lie with Windows or Mac, every operating system should be updated on a regular basis.

“One way the ‘bad guys’ get access to your system is to take advantage of vulnerabilities within installed software,” he explains. “By keeping your software up to date, you help to eliminate those vulnerabilities as quickly as possible.”

Reiman also says the number of **admins or individuals with login credentials should be limited**. The more admins a page has, the more

susceptible it is to threats. She encourages producers to play around with different ways to allow people access to a business's social media pages without granting everyone an admin level.

Malicious accounts with page names like "Verify Business Account Restricted" have resorted to tagging pages in posts. These pages claim violations have been detected and ask users to click a link to prevent their account from being deactivated.

Users are also receiving emails of a similar manner, where individuals posing as these social media platforms try to convince them that their posts and information will be deleted if accounts don't verify themselves immediately.

When unfamiliar emails or messages do come through online, Medsker says being suspicious includes checking the **subject lines and body context should carefully**. Misspellings and bad grammar are typically a red flag.

Though these messages can be alarming, Reiman urges producers not to panic or click any links.

"Usually if it sounds doomsday or uses words meant to cause alarm, such as 'immediately deactivate,' that is a huge red flag," she warns.

Companies like Apple, Google or Facebook will not reach out with an email or message asking users to login to verify your account. If there is concern, open a new browser window and navigate to the site personally before logging in and checking on the status of an account.

If an unexpected email claims to be from a familiar person or business,

Medsker suggests reaching out personally over the phone or to another trusted email. Only once the confirmation is received should links or attachments be opened.

If a link is included in a suspicious email, there are tools like **Google Safe Browsing to help verify we addresses**. A URL can be copied and pasted to check the status of the site.

Once a post or email is identified as illegitimate, report it or mark it as spam. Be sure to delete any lingering messages or notifications, so no one else accidentally interacts with the false information.

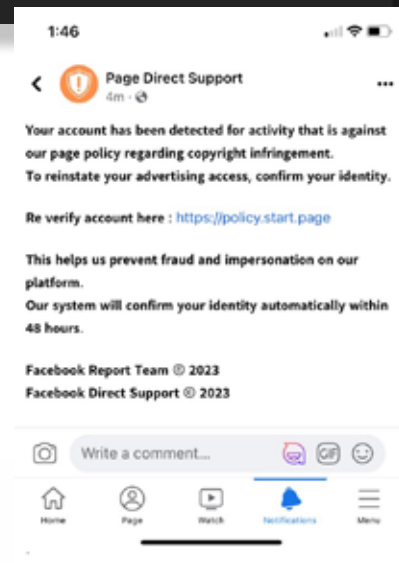
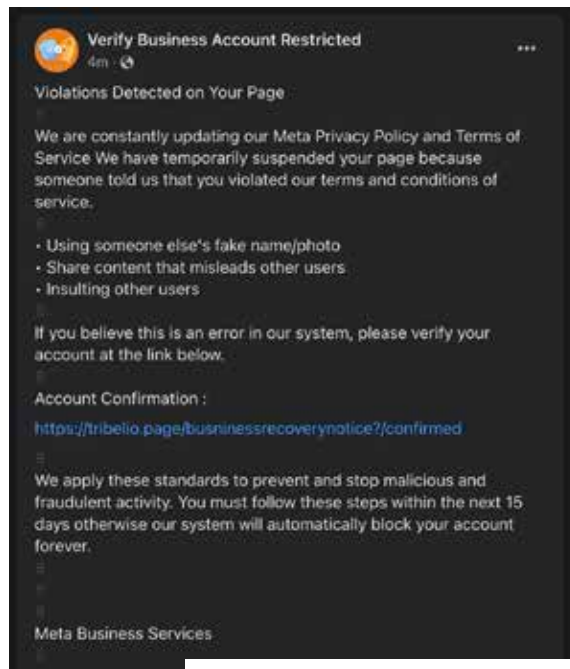
If unusual activity related to a social media page raises suspicion, Reiman suggests changing your password immediately and selecting the option to "sign out of all devices" when prompted. Report activity to the Help Center.

It happens more than you think

Meredith Terrell comes from a business and investment background, so she considers herself to be pretty cautious when it comes to helping her father, Tim, navigate "virtual" sales with Terrell Investments, Inc.

The North Carolina farm started selling registered Angus cattle in 2021, after COVID restrictions gave Tim enough time to return to his roots in the livestock industry. When

they received one of their first text messages about a party interested in purchasing a bull, the duo was eager to close the deal. The asking price was \$2,000, and the individual interested — "James Wright" — said he was only a few hours away from the Triad area where the farm was located.



Continued on page 48

Offers to visit the operation and see the bull in person were refused, and Wright even turned down free delivery for the bull. He insisted he was ready to complete the transaction and had a trucking service all lined up.

The strangest thing of it all? Meredith says he refused to communicate any other way than through text messages.

“It dragged on for a while,” she explains. “They would never talk on the phone, so I was getting suspicious.”

When the check came in the mail, things really started feeling strange to the family.

Though they asked for a certified check for the amount of purchase, it arrived instead with \$4,200 written as the total. Wright texted again, saying he had accidentally combined the price of the bull and the trucking fees. He asked the Terrells to cash the check, keep their original \$2,000 and give the remaining \$2,200 back to the trucker when he arrived to pick up the bull.

At this point, there was no doubt in Meredith’s mind this was a scam. She and Tim, however, agreed to see the interaction through just to see what would happen.

Continuing to text with Wright, Meredith offered to destroy the check so he could send one with the proper amount. His responses then became “aggressive,” as he accused the operation of trying to back out of the deal.

Doing some of her own research, Meredith looked up the address Wright had provided for his operation. The location was tied to an actual cattle ranch, but when she called the business, the manager she spoke to told her no one by the name of James Wright had ever

been employed there. Interestingly enough, however, the operation had fallen prey to an eerily similar scam just a few months prior.

Next, Meredith called the Kansas bank where the JPMorgan Chase check Wright has sent was from. The check was confirmed as a fake, but it was tied to the account of a real cable company.

After destroying the fake check, Meredith confronted Wright, telling him over text that she knew he was trying to scam her family. Despite her request to be left alone, Wright sent a few more aggressive messages, heckling Meredith in an attempt to convince her to finish the transaction.

Though the ordeal happened nearly two years ago, it’s still prevalent in Meredith and Tim’s minds as they continue to grow their business. The farm has advertisements online and in a few print publications, so a lot of business does happen virtually, but the pair has a few practices to help ensure the leads they’re pursuing are legit.

“Some of it is intuitive knowing,” she says, encouraging cattlemen to trust their gut when things don’t feel right.

Pay attention to the information a potential customer shares. Fairly early in the interaction, the individual should offer their full name, potentially an operation name and the location of their farm or ranch. Meredith says it’s important to **do some research** to help confirm the legitimacy of the interest.

A customer’s experience in the livestock world is also a good sign. Though experience isn’t a deal breaker, the Terrells say the individual should at least be asking some relevant questions — details about expected

progeny differences (EPDs), pedigree or Association membership.

Parties looking to purchase an animal should also possess land. Whether it’s leased or owned, Meredith says anyone looking to bring cattle home should have a place to house them.

The process of selling animals should not be complicated. If customers work on tight deadlines or insist on strange timelines, Meredith says cattlemen should take a step back. Wild or aggressive demands of when, where or how a purchase should be completed is never a positive sign.


When a contact is local, Meredith and Tim says it’s always a good idea to **invite the customer to the ranch or farm**. If there’s a chance of shared contacts, Meredith even suggests **reaching out to others to confirm the customer’s identity and interest**.

The biggest lesson —in combating both hackers and scammers — is to stay alert.

“I think just be careful,” Meredith says. “And remember...it’s okay to report it.”

With social media rising in popularity, the possibility of being hacked or targeted by a scammer is more prominent than ever before.

By simply reaching out to a regional manager or another staff member of the American Angus Association, Meredith says a producer can share their story and hopefully help another breeder in the future. The more visibility scams have, the fewer people that may get caught in them, Reiman says.

Social media and online commerce have changed the cattle business, with some extra effort it can be all for the positive. 

SCAN TO FOLLOW 
Angus Media on Facebook

