Stop Making Yourself Vulnerable Online

5 Simple Steps to Protect Yourself from Cybercrime

DARCY MAULSBY
JAN 31, 2024

Share

It's one thing to hear that global cybercrime is increasing every year, but it hits home when I learned that there's been a dramatic increase in cyberattacks in agribusiness, food production and farming in the past few years. While I wrote this story for Farm News, I'm sharing it here, too. Even if you're not a farmer, it's time to take cybersecurity seriously, according to Iowa State University (ISU) Extension.

"Cybersecurity is a team sport, and everyone has a role to play," said Doug Jacobson, an Iowa State University (ISU) professor of electrical and computer engineering and director of the Center for Cybersecurity Innovation and Outreach at ISU. "It's vital to control the things you can to protect your data. Don't be an easy target."

Keepin' It Rural is a reader-supported publication. To receive new posts and support my work, consider becoming a free or paid subscriber.

Type your email... Subscribe

Jacobson spoke at ISU Extension's Cybersecurity on the Farm conference on January 11 in Ames. A wide variety of speakers all agreed on one key point: cyber attackers are becoming more creative and are targeting sectors that are critical to human life, including agriculture.

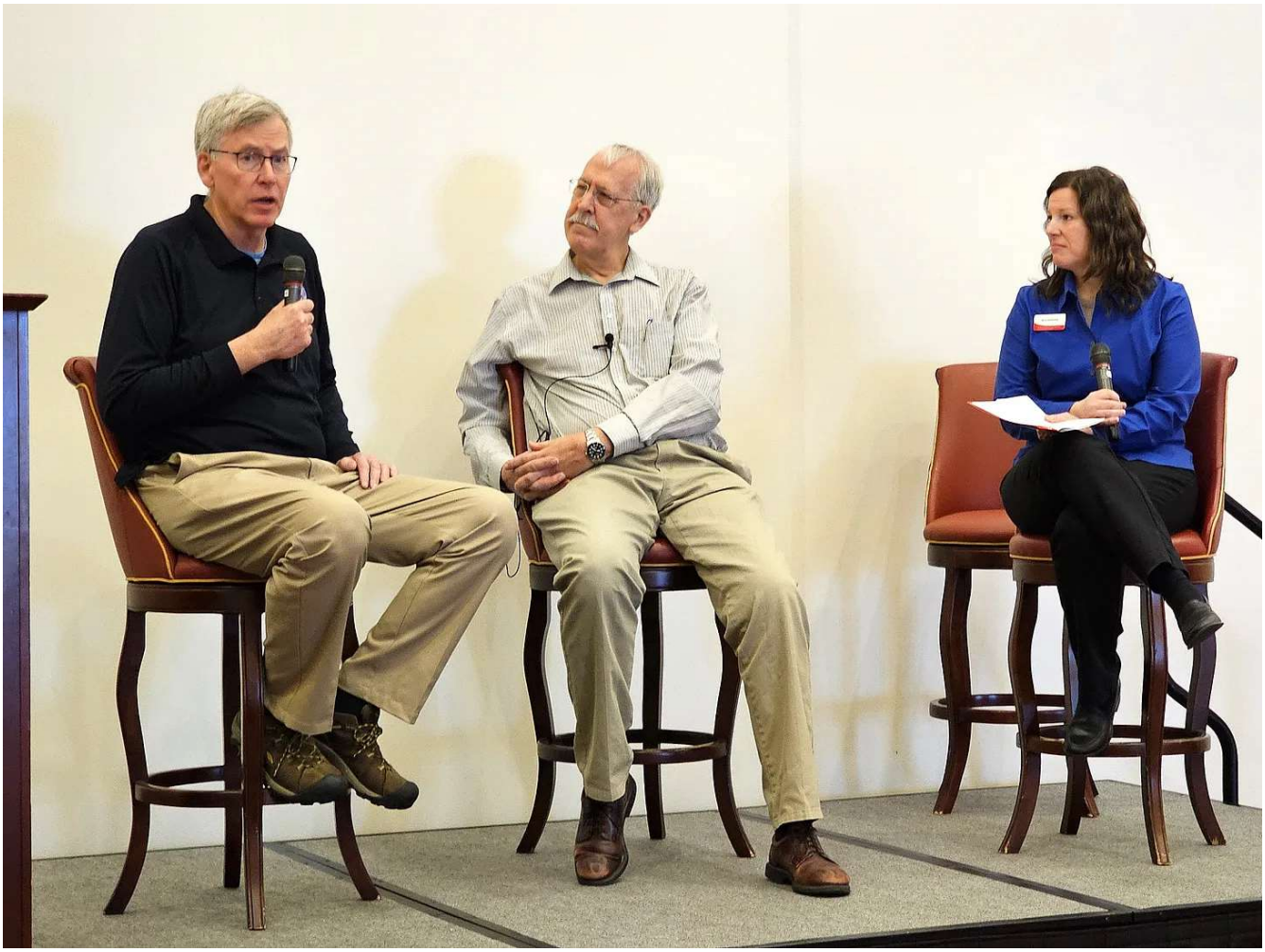
With 50 billion electronic devices connected to the Internet today, from smartphones to laptop computers to software in farm equipment, there are countless ways for attackers to strike. "Food and agriculture are critical to our nation's security," said James Hoflen, an advisor to the U.S. Cybersecurity and Infrastructure Security Agency. "That's why food and ag are specified among the 16 critical sectors defined by the U.S. government's Critical Infrastructure Security and Resilience Agency (CISA), America's cyber defense agency."

While cyberattacks are a computer issue, they really are a human issue. "Attackers use social engineering to target specific industries and people," noted the 2022 ISU Extension report "Everyone Has a Role in Cybersecurity." "Attackers use social engineering to target specific industries and people. Farming is a large part of that."

Social engineering is the tactic of manipulating, influencing or deceiving a victim to gain control over a computer system, or to steal personal and financial information. Social engineering uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

This can manifest as vague, ambiguous emails, for example, or extremely targeted messages. "An attacker may know where your farm is, where you shop and what supplies you need, so a targeted phishing email may look like an invoice for fertilizer or other supplies," according to ISU Extension.

That's why an important part of cybersecurity on the farm is cyber defense. "Don't be the person who stands out like a sore thumb and practically screams, 'Hit me!'" Jacobson said.



Protect yourself and your farm

Hoflen and Jacobson offered these five tips to boost cybersecurity on the farm:

> 1. **Beware of phishing attacks.** The most common form of a social engineering attack is phishing. Phishing attacks usually come in the form of emails that exploit human error to harvest data or spread malware, usually via infected email attachments or links to malicious websites. “If you get a suspicious-looking email from your co-op, for example, don’t click on any links it contains,” Jacobson said. “Also, let your co-op know you received this email.”
>
> 2. **Change the default password.** Never keep using the default password that comes with an electronic device or other software. Jacobson gave the example of cyber criminals who hacked into public waterworks systems in the eastern United

States, simply because the people running the waterworks kept using the default password that came with programmable logic controller (PLC) that operated the equipment. In addition, avoid using the same password on all your online accounts. It's also important to protect your passwords and keep them all straight, said Jacobson and Hoflen recommend using a password manager system. "Even writing the passwords down in a paper book is better than nothing," Jacobson added.

3. **Use multi-factor authentication.** This requires the user to provide two or more verification factors (a password and a special code that is texted or emailed to the user) to gain access to an online account. Think of multi-factor authentication like a deadbolt on the front door. The smaller lock on the knob might do the trick, but it's better to have an additional obstacle for criminals to overcome if they want to get in. Multi-factor authentication provides an additional lock on the doors to your online data.

4. **Don't think only certain age groups are vulnerable.** While older adults are often cautioned about online frauds and scams, younger people can also be at risk. It appears that more cybercriminals are more willing to go after smaller dollar figures, and they're willing to work harder to get the money, even if it's just $200 or $300, Jacobson said. "We're seeing a lot more targeted threats. The 18- to 25-year-olds have some of the highest median losses from these online scams, with a median loss of $177."

5. **Watch for red flags.** Beware if you receive an email from your bank or other company asking for your account number or social security number. "Your bank is never going to email you for either of those numbers," Jacobson said. Also, be very leery if the person or entity who is contacting you requests payment in cryptocurrency, wire transfers or gift cards. "Scammers today are sending multiple emails and are communicating back and forth with victims more, because it can be worth their time to craft these attacks this way," said Jacobson, who noted that cybercriminals posing as a government agency targeted an international ISU student and threatened the student with deportation. Unfortunately, the student got caught

> up in the scam and gave them $7,000 worth of Walmart gift cards.

If you get hit with ransomware, contact the Federal Bureau of Investigation (FBI),which has regional offices in Iowa and Omaha. “You want to keep yourself out of further trouble,” Jacobson said.

It’s hard to tell where cryptocurrency will end up. It could be going to a country that harbors terrorists. “Giving money to North Korea, for example, is a felony,” Hoflen said.

Reporting ransomware to the FBI has another advantage. “The FBI has an average retrieval rate of 70% of cryptocurrency in ransomware cases,” Hoflen added.

Since there are plenty of cybercriminals plotting scams, it’s worthwhile to focus on cybersecurity on the farm. Think of it like wearing a seatbelt, Hoflen noted. While it doesn’t removal all risk, it’s an important, simple step you can take to protect yourself. “You need to take reasonable precautions. Following a few simple, common-sense strategies can help keep you from being the low-hanging fruit when it comes to cyberattacks.”

Check out more Iowa stories from the Iowa Write Collaborative:

Nicole Baart: This Stays Here, Sioux Center

Ray Young Bear: From Red Earth Drive, Meskwaki Settlement

Laura Belin: Iowa Politics with Laura Belin, Windsor Heights

Tory Brecht: Brecht’s Beat, Quad Cities

Dartanyan Brown, My Integrated Life, Des Moines

Doug Burns: The Iowa Mercury, Carroll

Jane Burns: The Crossover, Des Moines

Dave Busiek: Dave Busiek on Media, Des Moines

Iowa Writers’ Collaborative, Roundup

Steph Copley: It Was Never a Dress, Johnston

Art Cullen: Art Cullen’s Notebook, Storm Lake

Suzanna de Baca: Dispatches from the Heartland, Huxley

Debra Engle: A Whole New World, Madison County

Arnold Garson: Second Thoughts, Okoboji and Sioux Falls

Julie Gammack: Julie Gammack’s Iowa Potluck, Des Moines and Okoboji

Joe Geha: Fern and Joe, **Ames**

Jody Gifford: Benign Inspiration, **West Des Moines**

Rob Gray: Rob Gray's Area, **Ankeny**

Nik Heftman: The Seven Times, **Los Angeles and Iowa**

Beth Hoffman: In the Dirt, **Lovilia**

Chris Jones, Chris's Substack, **Des Moines**

Pat Kinney: View from Cedar Valley, **Waterloo**

Fern Kupfer: Fern and Joe, **Ames**

Robert Leonard: Deep Midwest: Politics and Culture, **Bussey**

Letters from Iowans, **Iowa**

Darcy Maulsby: Keepin' It Rural, **Calhoun County**

Tar Macias: Hola Iowa, **Iowa**

Alison McGaughey, The Inquisitive Quad Citizen, **Quad Cities**

Kurt Meyer: Showing Up, **St. Ansgar**

Vicki Minor, Relatively Minor, **Winterset**

Wini Moranville: Wini's Food Stories, **Des Moines**

Jeff Morrison: Between Two Rivers, **Cedar Rapids**

Kyle Munson: Kyle Munson's Main Street, **Des Moines**

Jane Nguyen: The Asian Iowan, **West Des Moines**

John Naughton: My Life, in Color, **Des Moines**

Chuck Offenburger: Iowa Boy Chuck Offenburger, **Jefferson and Des Moines**

Barry Piatt: Piatt on Politics Behind the Curtain, **Washington, D.C.**

Dave Price: Dave Price's Perspective, **Des Moines**

Macey Shofroth: The Midwest Creative, **Norwalk**

Larry Stone: Listening to the Land, **Elkader**

Mary Swander: Mary Swander's Buggy Land, **Kalona**

Mary Swander: Mary Swander's Emerging Voices, **Kalona**

Cheryl Tevis: Unfinished Business, **Boone County**

Ed Tibbetts: Along the Mississippi, **Davenport**

Kali White VanBaale, 988: Mental Healthcare in Iowa, **Bondurant**

Teresa Zilk: Talking Good, **Des Moines**

Keepin' It Rural is a reader-supported publication. To receive new posts and support

my work, consider becoming a free or paid subscriber.

schultz@iastate.edu Subscribe

1 Like

Comments

Write a comment...

© 2024 Darcy Maulsby · Privacy · Terms · Collection notice
Substack is the home for great writing