UF IFAS Extension
UNIVERSITY of FLORIDA

UF/IFAS PEER REVIEWED

AEC755

https://doi.org/10.32473/edis-WC416-2022

Selling Safely: Cybersecurity Best Practices for Small, Rural Ag Businesses[1]

Lauri M. Baker, Cheryl R. Boyer, and Russell Boyer[2]

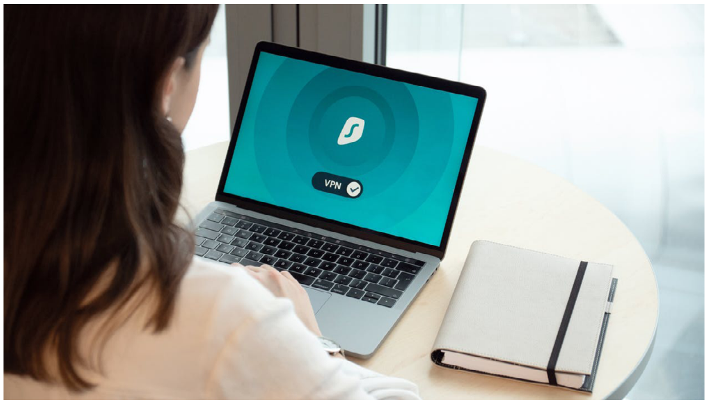

Figure 1.
Credits: Dan Nelson, https://www.pexels.com/photo/woman-using-macbook-pro-3949100

Cyberattacks are a continued and growing threat for all businesses. Small businesses, like agricultural and rural businesses, should not think they are immune to this threat: obscurity is not security. Small businesses may even be more at risk because they tend to have fewer practices in place to prevent a cyberattack. While attackers may prefer bigger, wealthier targets, they are also practical and may find multiple, small-scale attacks to be easier and less risky for them to complete (Alton, 2021). Make sure your business is prepared by implementing the best practices we have included here, and educate yourself using resources to which we have linked.

It is of the utmost importance for the continued viability of your business to protect your internet-connected systems from cyberattacks. It only takes one un-updated device or careless employee to open a window for attackers.

A study by Felton (2021) interviewed small business owners about cybersecurity practices and found that (1) small businesses perceived they had less of a security issue because of the size of the business, (2) they didn't perceive their business' data was valuable, and (3) they had limited education about cyber threats.

A survey from the Small Business Association indicated that 88% of small businesses were concerned about a cyberattack, but they lacked resources for technology support and/or lacked time and education related to cybersecurity (SBA, n.d.).

Types of Cyberattacks

The two most common types of attacks against small businesses today come from phishing and malware.

- **Phishing** is a type of social engineering attack delivered through email. Social engineering employs a combination of language, psychology, and specific knowledge to appear credible and manipulate people into taking action. Although some phishing attempts may appear to come from coworkers or others outside your company,

[1] This publication is AEC755, one of a series of the Department of Agricultural Education and Communication, UF/IFAS Extension. Original publication date May 2022. Visit the EDIS website at https://edis.ifas.ufl.edu for the currently supported version of this publication.

[2] Lauri M. Baker, associate professor, Department of Agricultural Education and Communication; Cheryl R. Boyer, associate professor, Extension specialist, nursery crop production and marketing, Kansas State University; and Russell Boyer, instructor, Department of Management, Kansas State University; UF/IFAS Extension, Gainesville, FL 32611.

phishing most often involves an email claiming to be from a credible source or authority. This email pressures the recipient into clicking on unsafe links, downloading files, or opening attachments with a demand for urgency on the recipient's part. Clicking on links or attachments may lead to the installation of malware on the user's system. However, most successful phishing attacks result in the user exposing secure credentials, such as user names and passwords, to the attackers. Employees in your business should be trained to recognize phishing attacks by watching for common clues such as generic greetings, poor spelling and grammar, suspicious sender email addresses, unusual requests, unknown attachments, and links to unrelated websites. While people can be trained to recognize most ordinary phishing attacks, others are much more difficult to spot. A "spear phishing" attack is a targeted attack that uses specific knowledge of its target to enhance its credibility and the chances of success. The target of an attack may be an individual, a department, a business, or a business's customers. Emails used in spear phishing attacks use familiar names, business logos, formatting, and fonts to mimic legitimate communications. For this reason, sophisticated spear phishing attacks can be very convincing even to the experienced eye. Although more difficult to detect, trained users are more likely to recognize the subtle inconsistencies typical of a spear phishing email.

- **Malware** is an umbrella term for a wide array of malicious software that can interfere with the normal function of your business' computers. Regardless of its specific intent, all malware compromises the security of your computing systems. Any malware, however benign, may be used to deliver other more disruptive (and potentially destructive) malware. Some of the most common disruptions from malware include slowed computer performance, redirection of browsers to unrequested websites, displaying unwanted advertisements, and the unauthorized collection of sensitive data. Examples of sensitive data include usernames, passwords, account numbers, payment card numbers, and social security numbers. Sensitive data collected by attackers may be used to compromise other systems within your business, to target your customers with spam or phishing emails, or to attack the systems of other businesses to which you provide a service. Perhaps the most destructive type of malware encountered today is ransomware. Ransomware encrypts the files on a compromised computer, rendering them inaccessible until a ransom is paid to the attackers. Ransomware attacks have proven to be some of the most profitable for cybercriminals and among the most devastating for businesses. In 2020, the Federal Bureau of Investigation's Internet Crime Complaint Center reported 2,474 ransomware complaints with adjusted losses of over $29 Million. Ransomware can find its way onto a computer through multiple vectors, including malicious files downloaded from websites, systems compromised through other malware or stolen credentials, or as a file attachment sent through email. Some ransomware applications may even spread automatically from a compromised computer to other vulnerable computers through your office network. After the ransomware has begun to encrypt the contents of the computer's drive, users will be unable to access their files and presented with a window detailing the demanded ransom and payment methods. Once a computer has been encrypted by ransomware, little can be done to recover the data. Thorough, secure backups of your critical business data are the most reliable method to protect your business from a ransomware attack. If vital data is lost to a ransomware attack, it may be necessary to pay the ransom. Agreeing to pay the ransom does not guarantee the recovery of your data, however. You are trusting that in return for the paid ransom, the cybercriminals will provide you with the cryptographic keys needed to recover your data.

Best Practices

We have compiled the seven best practices from across popular and research-based information on cybersecurity:

1. Have a cybersecurity plan.
    - Taking time to plan for a possible cyberattack can save you a lot of trouble in the future. Once a compromised system has been detected, a rapid response can be key to limiting or preventing the loss of your data.
    - Cybersecurity can be complicated, but the Federal Communications Commission has a planning guide specific to small businesses. Take some time to read it and create a plan for your business.
2. Educate yourself and your employees about cybersecurity.
    - Gather your employees for an initial discussion about the importance of cybersecurity and how you plan to address it.
    - Provide, and require, regular cybersecurity training to improve your and your employees' ability to recognize potential threats and act accordingly.
    - Make it everyone's job to be a part of the cybersecurity planning and process. This may require a shift in culture for your business if this has not been a priority before. Like any culture change, this will take time, but

it is an important part of making your business secure from cyberthreats.

3. Use anti-malware software and keep it updated.
    - There are many options available online. Explore your options and make sure you have anti-malware software on all work devices. Make sure you have all computers set to update the software automatically.
4. Store or back up your data using cloud storage.
    - Reputable cloud storage vendors have high security standards and built-in safeguards to protect your data from loss due to a cyberattack.
    - Cloud storage is often more affordable for small businesses than investing in your own hardware to store and back up your business' data.
    - Cloud storage solutions (like Dropbox or OneDrive) also include tools that make file sharing and collaboration easier.
    - If file sharing and collaboration are not needed, there are affordable cloud backup services that can maintain online backups of your data in case of catastrophic loss.
5. Passwords matter!
    - Access to all computers and Wi-Fi networks should require a password.
    - Passwords should be a minimum of eight characters in length and complex enough that it would be difficult for an attacker to guess or otherwise discover them (Grassi et al., 2017).
    - Learn more about creating strong passwords at https://www.businessnewsdaily.com/5597-create-strong-passwords.html.
6. Commit to regular updates and upgrades of software, computers, and malware protection.
    - When updates or patches to existing software are released, it is often in response to known bugs or a newly identified security threat.
    - While older versions of software may remain functional for your business, they may not receive security updates from the vendor.
    - Make time in your and your employee's schedules to regularly update software. Updates to software and operating systems can often be scheduled to occur outside of active business hours.
7. Protect your data.
    - Evaluate who needs access to information. If someone does not *require* access to all data to do their job, then limit their access to what they actually need.
    - Check with your bank and/or credit card processor to make sure you have the most up-to-date anti-fraud services.
    - If possible, have a dedicated device that collects payments. Ideally this device would not be one you use to search the Web.

Summary

While protecting your business from cybersecurity threats may not seem like an urgent need amid the tasks of your agricultural business, it grows increasingly more so in our highly connected society and business environment. Well-managed systems do not guarantee safety, but preparation and well-trained staff are essential to protecting your business and getting back up to speed in a minimal amount of time. Be prepared and, hopefully, you'll never experience a regrettable cyberattack.

References and Resources

Alton, L. (2021). *The 8 best cybersecurity strategies for small businesses in 2021.* INC.com. https://www.inc.com/larry-alton/the-8-best-cybersecurity-strategies-for-small-businesses-in-2021.html

Cybersecurity and Infrastructure Security Agency. (2020, August 25). *Security tip (ST04-014): Avoiding social engineering and phishing attacks.* CISA. Retrieved March 11, 2022, from https://www.cisa.gov/uscert/ncas/tips/ST04-014.

Federal Bureau of Investigation Internet Crime Complaint Center. (2020). *2020 internet crime report*. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Federal Communications Commission. (n.d.). *Cyber security planning guide*. https://transition.fcc.gov/cyber/cyberplanner.pdf

Felton, J. H., Jr. (2021). *Cyber resilience of small business owners* (Order No. 28318819) [Doctoral dissertation, Capella University]. ProQuest Dissertations & Theses Global. https://www.proquest.com/docview/2504819573

Grassi, P. A., J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Picher, N. B. Lefkovitz, J. M. Danker, Y.-Y. Choong, K. K. Greene, and M. F. Theofanos. (2017). *Digital identity guidelines: Authentication and life-cycle management.* US Department of Commerce National Institute of Standards and Technology, Special Publication 800-63B. https://doi.org/10.6028/NIST.SP.800-63b

US Small Businesses Association (SBA). (n.d.). *Stay safe from cybersecurity threats*. https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats