

Under lock and keyboard



All you need to know about protecting yourself in the digital world





Technically speaking
our language ▶

Small classes, hands-on learning and tuition you can handle. Learn more at bismarckstate.edu.

DISCOVER
THE NEXT VERSION
OF YOU





BSC cybersecurity offerings meet global crisis and urgent workforce need

Cybercrime is a worldwide crisis. Identity theft, data breaches and credit card hacking affect all of us – personally and professionally. The cost of cybercrime damage is expected to hit \$6 trillion annually by 2021.

As the problem grows, so too does the workforce need. More than 1.5 million unfilled cybersecurity positions will exist by 2020 – thousands in North Dakota alone. From a power plant in Beulah to a school district in Chicago to a bank in Fargo – cybersecurity jobs are diverse and vital to the wellbeing of society.

in this exciting and lucrative field. We offer certificate, two-year and a four year degrees in Cybersecurity and Information Technology. And, as the higher education lead in North Dakota Governor Doug Burgum's K-20W cyber initiative, our partnerships across the state and nation, create guaranteed paths to a secure future. Learn more about BSC's cyber and computer offerings at bismarckstate.edu/cyber.

BSC Cybersecurity partners Palo Alto Networks, Midco, NISC and Great River Energy.

BSC opens the door to a career

BBB of Minnesota and North Dakota Names Top Scams of 2018

Burnsville, MN – March 6, 2019 – Better Business Bureau of Minnesota and North Dakota (BBB) has compiled a list of the Top Ten Scams of 2018 that were reported to BBB's Scam Tracker. Online purchasing scams had the most reports out of the more than 900 reports filed last year in Minnesota and North Dakota, followed by phishing and employment scams. Employment scams topped off the list of the more than 50,000 scam reports published in the United States and Canada.

Most of the online purchasing scams involved a buyer ordering and paying for an item and never receiving it. These items include automobiles, pets, tickets, clothing, and cosmetics. The items are often found for sale on sites such as Craigslist, eBay, Facebook, and other direct seller-to-buyer sites. Online purchasing scams came in at number two in 2017.

Top Ten Scams of 2018 in Minnesota/North Dakota:

- Online Purchases
- Phishing
- Employment Scams
- Credit Card Scams
- Social Security and Tax/IRS Collection Schemes

- Tech Support Scams
- Debt Collection Scams
- Fake Check/Money Order Scams
- Counterfeit Product Scams
- Fake Invoices
- Top Ten Scams of 2018 in the United States/Canada:
- Employment Scams
- Online Purchases
- Fake Checks/Money Orders
- Home Improvement Scams
- Advanced Fee Loan
- Romance Scams
- Tech Support Scams
- Investment Scams
- Travel/Vacation Scams
- Government Grant Scams

BBB Scam Tracker was launched in North America in 2015. Since that time, it has received nearly 150,000 reports of suspect offers, fraud or attempted fraud. BBB staffers review all submissions to the site in order to watch for patterns of a problem and ensure the submissions are authentic. Reports that involve legitimate businesses are converted to complaints. Scam Tracker also gives people the ability to see where scams are occurring locally and nationally and allows them to search for fraudulent activity by keyword or within geographic regions.

Even if consumers or busi-

ness owners don't fall victim to schemes they're confronted with, they're encouraged to file a report through BBB Scam Tracker. Data collected through these reports is compiled and shared with law enforcement who, with enough information, may be able to take steps to shut down fraudulent websites and illicit operations.

For the full report, go to BBB.org/RiskReport

To report a scam, go to BBB.org/ScamTracker

To learn more about different scam types, go to BBB.org/ScamTips

Media Contact: Bess Ellenson, Communications Director
651-695-2463 / bess.ellenson@thefirstbbb.org

With more than 7,200 regionally Accredited Businesses, BBB of Minnesota and North Dakota is a not-for-profit organization. The mission of BBB is to promote, through self-regulation, the highest standards of business ethics and conduct, and to instill public confidence in responsible businesses through programs of education and action that inform, protect and assist the public. Contact the BBB at bbb.org or 651-699-1111, toll-free at 1-800-646-6222.

Health careers get the full treatment at BSC

As the nation struggles with a shortage in healthcare workers, Bismarck State College is not only graduating work-ready nurses, medical lab techs, surgical techs and paramedics, the college is expanding to create more opportunities for people to enter this growing field.

Statistics

In 2018, the healthcare industry reported the largest number of job openings

From 2016-26, North Dakota will see a nearly 20 percent increase in healthcare jobs

North Dakota currently has 1,938 healthcare-related job openings

Graduates from BSC Health Science programs routinely achieve pass rates of 96 to 100% in national exams for nursing, surgical technology, medical lab technician and paramedics

In order to meet demand in this field, BSC is in the midst of a two major initiatives.

Moving Health Sciences programs moving to main campus

BSC Health Sciences will be moving to the main campus this summer, allowing the programs to grow by creating a permanent home as the lease will soon end on the programs' current downtown training facility.

The new space will accommodate more students, and offer state-of-the-art-technology and the equipment to prepare for the healthcare jobs of the future. A virtual hospital will be created in the facility to allow innovation and collaboration between the programs, providing more training opportunities in Nursing, Surgical Technology, EMT/Paramedic Technology, Medical Lab Technician and Certified Nursing Assistant programs.

Bringing training to your community

BSC recently purchased a rov-

ing simulation lab for their students training to be nurses at the college's satellite sites in Hazen, Harvey, Ashley, Garrison and, starting next fall, Hettinger.

In the past, those students had to travel to Bismarck to train with the simulations. Annie Paulson, director of BSC's nursing program, says this will ensure students at the BSC satellite sites are receiving the same quality of education as the students in Bismarck, as well as help recruit nurses in rural areas where there are often shortages.

"The healthcare industry has huge demand for workforce right now, and employment projections show that demand will continue to grow," said Dr. Larry C. Skogen, BSC president. "We are poised and ready to meet this ever-growing need"

For more information on BSC's Health Sciences programs visit, bismarckstate.edu.

On-Farm & Off-Farm Custom Slaughtering

We are here for all your slaughter needs



WHERE SERVICE & EXCELLENCE MEET

Call us to reserve your slaughter spot today!

Formerly 2K Meats
Same People, New Name

713 Hwy 49 N, Beulah, ND
873-2566

April Showers of Savings

Free
digitizing on pocket logo

40% Off
Winter Stock
hoodies, jackets, hats, long sleeves

25% Off
New order

20% Off
Any speciality item order
pens, mugs, banners

10% Off
embroidery on stadium chair

VIKING Screen Prints

Mention this offer. Limit one offer per purchase. Some exclusions apply. Expires April 30, 2019



Locals avoid internet scam

By Suzanne Werre

Most folks are familiar with the adage “caveat emptor,” which means buyer beware.

Fewer are familiar with the “cave venditor” – seller beware.

Underwood’s Kellie and Leon Weisenburger recently became even more aware of how important it is for the seller to beware, as they recently made a sale for a used direct drive for a boat on BisManOnline – even getting the \$4000 price they asked for without any haggling.

It was the “no haggling” that rang one cautionary bell to the Weisenburgers that made them question the validity of the offer.

“He didn’t dicker on price or anything,” he said. “Nobody does that.”

They quickly received an email from “PayPal” that looked pretty official – legitimate -- said Weisenburgers. But what it said seemed a little suspicious.

The email they received from “PayPal” said that PayPal had received the payment of \$5000 from “Mark Houts,” but that it would not be reflected in the Weisenburgers’ account until after they sent \$900 through the “Nearest WesternUnion store” to the transport company (to pay for shipping).

Them having to pay shipping on the item they were selling was just more proof that they were being scammed.

The seller should never be sending the buyer any money for shipping, noted Leon.

The communication between the Weisenburgers and the “buyer” lasted about two days, with the buyer sending several texts.

They received emails from “PayPal” . . . and the FBI.

After the Weisenburgers informed the buyer they were rethinking the transaction, they got an e-mail ostensibly from the FBI indicating the feds were aware of the transaction, threatening to arrest them because they had not sent the \$900.

The fact that the email was from the “Federal Bureau OFF Investigation,” added more evidence to their suspicion of a scam, and the fact that the email came from a gmail account only confirmed their suspicion.

“First of all, the FBI isn’t going to threaten to arrest you over email,” said Kellie. “These people just try to put a little bit of fear into you. It’s just a big scam.”

“It’s probably a guy sitting on a beach doing all this stuff from his laptop, just scamming \$900

from people,” said Leon.

Kellie called PayPal directly after they got the first email saying they had \$5000 waiting for them in their account once they paid the \$900 shipping, and she was told there was no pending \$5000 payment.

“They said no, that’s not how we work,” said Kellie.

Again, they noted, the emails

“It’s probably a guy sitting on a beach doing all this stuff from his laptop, just scamming \$900 from people.”

-Leon Weisenburger

looked pretty legit, with a PayPal-type logo on the top and pretty convincing text.

People need to be aware this type of thing is happening all over to all sorts of people – young and old, she said.

The Weisenburgers contacted BisMan to let them know about the scam attempt, and they were told it’s a known scam, and there’s nothing they can do about it. The bad thing is there’s really no way to track the scammers because most of the time the scammers are using a phone that they get rid of after they’ve made some money.

“Usually it’s a throw-away phone and they’re doing a few transactions on it, and when they start getting some heat, the phone is gone,” said Leon.

During this, they also got an email, ostensibly from BisManOnline, warning them that their account had been hacked and that after they verify that they are the owners of the BisMan account, they would send them a link which would allow them to change their password and install a “new Upgraded Security Link.”

It was just another part of the scam that could have given the scammer even more access to the Weisenburgers’ information.

The Weisenburgers contacted Detective Justin Krohmer with the McLean County Sheriff’s Department, and he reiterated BisMan’s contention that there’s no way to track the scammer to find out where he or she is.

The IP address that belongs to this scammer is from Uganda, but that’s all they know.

Kellie wants to warn people about the possibility of scams.

BisManOnline and PayPal are well known and respectable businesses, and it would be easy for

someone getting an email from them to believe it’s legitimate.

“Again, you just have to look at the email address and you know that it’s not right,” she said.

They caught the red flags, so they didn’t lose any money, but they want to remind people to beware.

The email address is a sign, and an even more obvious sign is if someone asks the seller to send them money first.

“If you’ve got suspicions, ask someone,” said Leon. “Ask people, ask questions. Ask somebody for help or call and verify that that is their procedure. You should never have to send any money or pay a company to ship it – that should all be handled on the buyer’s end.”

The take-away from this experience – beware, and don’t be afraid to ask questions.

PayPal questions and answers

Follow the verification procedures below and send us the requirement so we can release the fund to your account.

Dear PayPal User,
Kellie Weisenburger

This is to inform you that we have received the payment of \$5,000.00 USD from Mark Houts for the Merchandise bought from you and the funds will only reflect in your account after all due measures have taken place In order to complete this transaction, You will have to go to a Nearest Western Union store with \$900.00 USD cash and send to the Transport Company out of your pocket before you can have access to the whole payment, We advice you to go to the nearest Walmart office in your area and get back to us with the Scanned Copy/Photograph of the Western Union Money Transfer transaction receipt or send us the REF # including the sender name, address, As soon as we have received this information from you, we will credit a sum of \$5,000.00 USD to your PayPal account.

Below are some frequently asked questions to help you understand fully.

Q 1. I am the seller, why do I have to send my money upfront to the shipper to get my money released?

Sending money upfront to the shipper by the sellers to get the funds released is a new protocol organized by PayPal security team to enhance fast, smooth and secured transaction. Because in last few years, we usually release the total funds to the sellers account and request them to send out the added fee to the shipping company immediately, but we noticed most of the sellers will not send it instantly, some might take days and this usually delays the shipping processes. Some seller will even transfer the

whole funds out and deactivate their PayPal account after they have gotten the whole money and disappear, we have no choice than to refund the buyer and this is becoming a great loss to our company so we created this protocol to help guard you & your buyer from losing money. So you are secured.

Q 2. Why did my buyer send the shipping fee to my payment and why can’t my buyer send the shipping fee to the shipper themselves?

The main reason we debited your buyer’s account with the shipping fee and didn’t let them send it to the shipper themselves is that, in PayPal rule and in a transaction like this, it is the sellers responsibility to send the shipping fee in their name to the shipping company so they can have the copy of the payment receipt for reference to show the shipper whenever they show up for the pickup.

Q 3. Is there any assurance that I will be fully credited once I send the shipping fee out of my pocket?

Of-course yes, you are 100% guaranteed over this transaction and all mails are being monitored by the FBI so no need for you to panic you will be fully credited immediately. PayPal is all about secured payment. We are a trusted company in the world. We understand how important security and peace of mind are in the online business, so rest assured...

All you have to do is to reply back to this email with the western union money transfer details of the money sent for verification. Once it has been verified, you will receive a “CONFIRMATION EMAIL” from PayPal® Service informing you that your account has been credited.

Thank you for being an asset to PayPal.



DON'T SKIMP ON SECURITY.

Cybersecurity and identity theft are real. Protect your devices, your data, and yourself! Make sure that your devices are all up to date and have valid anti-virus software. Your passwords must be kept safe and changed frequently. Contact us if you suspect any suspicious activity.

A Better State of Banking



Member
FDIC

877.684.2233 | BetterState.com

Did you know?

All BEK Lightband subscribers get 50gig of FREE storage on BEK Cloud Backup to help you keep your data safe and private.

BEK Cloud Backup features:

- ✓ Advanced Encryption
- ✓ Hometown service & support
- ✓ Unrivaled transfer speeds
- ✓ Protect important documents
- ✓ Archive precious family photos

Call 888.475.2361 to activate your free 50gig of BEK Cloud Backup storage today



BEK Lightband, Gigabit Internet Service, available as standalone starting DECEMBER 1, 2017. Some restrictions may apply, limited to BEK Services area.

Garrison State Bank and Trust has you covered

Security

Garrison State Bank and Trust understands that your trust in us depends on how well we keep your personal, business and account information secure.

Our **Customer Information Security Policy** is comprehensive, proactive and designed to ensure that information about you is secure whether you bank with us at our main location, at our ATMs, or by telephone or Internet.

We will continually update and improve our security standards to help protect against unauthorized access to our confidential information. We will maintain physical, electronic and procedural safeguards that comply with federal standards to guard customers' information.

Padlock Website Security Padlock

In order to protect the information being gathered, this site has security measures in place including firewalls, encryption, and authenticated access to internal databases where needed.

We provide Internet access to your banking accounts through highly secure, password-protected systems that are guarded by firewalls and monitoring systems. Your financial information is protected by 128-bit encryption as it travels between our servers and your computer.

Look for security certificates, locked padlock symbols and the https: designation as indications of our commitment to your online security.

Multi-factor Authentication and Layered Security

When you bank online, you'll notice some new processes having to do with how you identify yourself and gain access to your accounts over the Internet. These processes are designed to make you safer than ever before from identity theft.

Today's authentication methods--used to confirm that it is you, and not someone who has stolen your identity--involve one or more basic factors:

- Something the user knows (password or PIN)
- Something the user has (ATM card or similar item)
- Something the user is (biometric characteristic, such as a fingerprint)

Single-factor authentication uses one of these methods; multi-factor authentication uses more than one, and thus is considered to be a more reliable and stronger fraud deterrent. When you use your ATM, you are using multi-factor authentication: Factor number one is something you have, your ATM card; factor number two is something you know, your PIN.

Garrison State Bank and Trust's goal is to ensure that the level of authentication used in a particular transaction is appropriate to the level of risk in that application. Accordingly, we have concluded an assessment of our current methods following federal regulatory guidelines and will be implementing the appropriate authentication measures to keep your online transactions safe and secure.

In addition to single and multi-factor authentication, we may also rely on layers of control to assure your Internet safety. These might include:

- Additional controls, such as call-back verification
 - Employing customer verification procedures, especially when opening accounts
 - Analyzing banking transactions to identify suspicious patterns
 - Establishing dollar limits that require manual intervention to exceed a preset limit.
- One of our top priorities is to assure your safety and security when conducting online financial business.

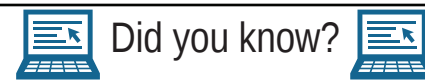
Customer Awareness

Understanding the risks is a critical step in protecting yourself online. Here are some threats to watch for:

Phishing --Lures you to a fake website (one that looks like a trusted financial institution) and tricks you into providing personal information, such as account numbers and passwords.

Pharming --Similar to phishing, pharming seeks to obtain personal information by directing you to a copycat website where your information is stolen, usually from a legitimate-looking form.

Malware --Short for malicious software, often included in spam e-mails, this can take control of your computer without your knowledge and forward to fraudsters your personal information such as IDs, passwords, account numbers and PINs.



Ransomware is a form of malware (malicious software) that takes over a computer. Ransomware can lock down all operations on a computer and deny users access to their data.

Computer users cannot reverse this lock down without the help of the hacker, who usually requires a ransom in return for a decryption key. The costs can range from a few hundred dollars to thousands, say IT experts. The U.S. Department of Education has warned that hackers are employing ransomware as they target schools with insufficient security.

According to the Federal Bureau of Investigation, schools are particularly vulnerable because their security is not always up to par and they have information that's of value to hackers, including students' personal information.

According to McAfee, more than four million ransomware variants have been detected online, a 270 percent increase since 2013, and ransomware is expected to be a continuing and significant problem for schools

C-Ram

Sales & Service
Virus & Malware Removal
Data Recovery
Hardware Upgrades
Avast Business Security

701-223-3109

1401 South 12th Street Bismarck ND 58504

Online Banking

Enroll | Forgot Password

Products & Services
Online & Mobile
Trust Services
Resources
About Us

Your money security is our top priority.

Here are a few tips for protecting yourself online:

- Never share your access codes with anyone.
- Change your access codes on a regular basis. If you think your access codes have been compromised, change them and contact us immediately
- Use only the secure message service provided within NetTeller Online Banking when sending or requesting account information.
- Consider using a personal firewall to prevent hackers from invading your personal computer, especially if you are using DSL or a cable modem to access the Internet.
- Install virus protection software and scan all downloaded software. Also, delete e-mails with attachments from unknown sources.
- When you are done with your transactions, always click on the Logoff button on the website to exit the application and prevent further access to your account.

Garrison State Bank & Trust

Community Banking at its Best

463-2262 • Garrison, ND | 679-2140 • Max, ND | www.GarrisonState.bank

CENEX



1600 Hwy 49 N, Beulah • 873-4363
211 E Main St, Halliday • 938-4716

BEULAH & HALLIDAY

Your Local Area Source For Feed Supplements, Seed, Fertilizer & More!



PAYBACK

Authorized Dealer



MINERAL

We Deliver!

Complete line of cattle, equine, swine, goat and poultry feeds & minerals.

CENEX AGRONOMY CENTER!

Locations in
Beulah & Halliday



Farmers time is valuable and we value that in our company!

You can call ahead and we will work with you to have your fertilizer ready to load when you arrive!

We Have What You Need To Grow!

- Bulk Dry Fertilizer
- Custom Fertilizer Application
- Liquid Fertilizer
- Anhydrous Ammonia
- Bulk & Packaged Chemical
- Crop Scouting

We offer custom fertilizer application!

We have 2 fertilizer spreaders (and offer variable rate technology) to ensure the job gets done quickly!

The size of our plant helps us buy fertilizer to keep prices competitive!

Fertilizer Plant 873-5999

Tim Loen, Agronomy Manager 891-1867

Ron Berg, Salesman 880-2014

Dyllon Schnaible, Salesman 873-7730

Both locations offer fertilizer blending capability and NH3 nurse tank filling

How to Protect Yourself from Online Scams

Be alert. Know that anything you do online has the potential for danger. That includes many actions that seem innocuous, like clicking a link in an email you think was sent from a friend, providing personal information on what looks like a legitimate retailer's site, or opening login details to a friendly person who calls you to talk about a software upgrade.

Trust your gut. If anything looks, sounds, or feels suspicious, take a step back and think before you act. For example, if you get a Facebook invitation from someone you're already friends with, check with them through another channel (such as text message or email) on whether or not it's a legitimate request. If someone calls from a company you've never heard of to "x" your perfectly functioning computer, hang up.

Ignore random notifications. Flashing notifications saying your computer has a virus and you need to download software immediately to fix it can be alarming. But that's exactly how they're designed. Don't trust pop-ups or other notifications from unknown sources. If you're genuinely concerned there's a problem with your computer, run a virus scan or take it to a professional who can help.

Protect your personal data. Be very wary about any requests for personal information such as your Social Security number, mother's maiden name, or passwords. Practice cyber-hygiene. Just as you brush your teeth, get a good night's sleep, and exercise to stay healthy, you need to perform certain tasks to ensure your online health is maintained. They include always using strong passwords and keeping them secret, installing and updating security software, backing up content, and not using Wi-Fi in public places for sensitive transactions (such as banking).

Secure your social media. All social media applications have security and privacy settings you can adjust. For example, Facebook asks for your email address and phone number, but it's optional. Sure, it might be a little harder for friends to get in touch with you if you don't provide these items, but remember that anything that makes you more accessible to friends also makes you more accessible to scammers.



LIVE YOUR BEST INTERNET LIFE.
Because you matter.

Get More Protection with Tech Home

Tech Home Protect Plus Support is technology made easy - a variety of managed solutions available from RTC to handle your Internet Security and data storage. They include:

- **SecureIT Plus** - Provides real-time protection against viruses, ransomware, and a host of other common threats.
- **FileHopper Plus** - Lets you back up your most important files and photos with 250 GB of backup space.
- **Password Genie** - Stores your passwords in one secure location and can generate strong passwords for you.
- **Identi-Fi** - Enables you to identify where you have a low Wi-Fi signal and know who and what devices are connected to your network.

You can enjoy the peace of mind of having some of the Tech Home services for as little as \$5.95/mo. If you sign up for RTC's Ultimate Whole Home Wi-Fi Package, it includes the entire Tech Home Protect Plus Support package at no additional charge.

To learn more, visit
www.RTC.coop/wifi
or call **888.862.3115**



RTC wants to help you protect yourself from hackers

Follow these tips to reduce your odds of becoming a victim

With so much hacking going on, it may feel like it's only a matter of time before you become a victim. Fortunately, you can often outsmart the hackers by following these tips:

Follow Up After Attacks

If a service you use is hacked, the first thing you should do is change your password. If you use the same password on other accounts, change them as well. Then, check the account to see if anything looks amiss. If it does, contact the service to see how they can help; depending on the type of service, you may also want to shut it down. Check your financial statements and

credit report carefully to ensure your private information hasn't been used to break into other accounts.

Use Good Password Hygiene

When creating new passwords, use a different one for each service. Be especially careful not to use the same passwords for bank accounts, email, and eCommerce accounts. Change your passwords at least once a year, on a date that's easy to remember, such as January 1. Consider using an online password service like LastPass or Dashlane to conveniently and safely track passwords.

Freeze Your Credit

If you're the victim of more than one breach, you might want to freeze your credit, which involves disallowing anyone from viewing your credit reports, making it more difficult for anyone to open an account in your name. To learn more, visit the Federal Trade Commission section on the topic at consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Log In the Right Way

More companies are now using two-factor authentication, which requires you to use a secondary password if you log in from an unrecognized device. If you have

the option to use two-factor authentication on a service, do so. In addition, always check for the padlock icon next to the URL to ensure the services you use are secure.

Protect Your Computer Network

Set your computer to update your operating system automatically, which prevents hackers from taking advantage of vulnerabilities in outdated programs. Likewise, make sure your anti-virus and anti-malware programs are always up to date. When setting up Wi-Fi in your home, be sure to protect it with an en-

rypted password and update your hardware every few years.

Don't Forget

About Your Phone

Remember that your phone is a computer too, and hackers can get a lot of personal information from it. Phones are easily lost or stolen, so if yours has a way to be locked, use it! Develop a numeric code with the highest number of digits allowed (four is great, six is even better) or use the fingerprint sensor if your phone is so equipped.

Remember, hackers can't see what they can't see, so keep your data behind closed (cyber) doors.

Worldwide cooperation needed to improve cybersecurity

By Francisca Afua Opoku-Boateng

MADISON, S.D. – Information is power, and cybersecurity is all about protecting that information to make it as secure as possible. This is important whether you live in the United States or in any country around the world.

Ghana, my home country in West Africa, is not immune to cyber risks and attacks. Electronic payments and commerce fraud, "sakawa" or internet fraud, ransomware, insider threats and identity theft, social media abuse, social engineering, web defacement and ATM fraud are top cybersecurity issues.

Plus, Ghanaian news and media outlets have reported that cybercriminals are getting smarter by the day, sharpening their skills and discovering innovative ways to gain access to networks and data of businesses such as financial institutions. A report released by a Kenyan-based IT firm, Serianu Ltd., revealed how the Ghanaian economy lost a total of U.S. \$50 million to cyber-crime in 2016.

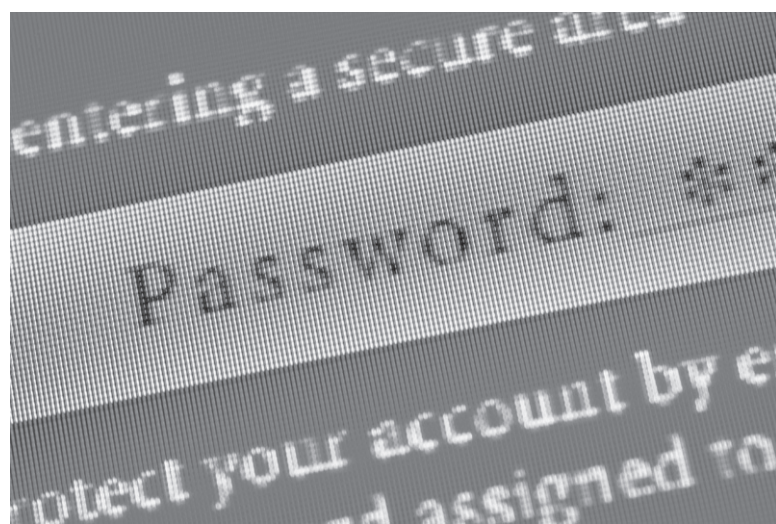
Ghana is taking baby steps with cybersecurity. For example, in Ghana there was no proven system for monitoring cybersecurity developments, and the International Telecommunication Union of the United Nations observed the absence in the country of a national governance roadmap for cybersecurity, although Ghana had a drafted national cybersecurity policy. That policy seeks to address the lack of awareness of risks that users and businesses face when doing business in cyberspace.

Leaders have recognized the need to develop a technology framework for combating cyber-attacks. So, Ghana's vice president recently launched the 2018 National Cybersecurity Awareness Program, which calls for the intensification and harmonization of efforts to fight cybercrime and control or limit the increasing danger.

Institutions such as the Bank of Ghana are putting measures in place to fight cybercrime, part of the government's push to beef up security and protect the country's business institutions from cyberattacks.

Combating cyber threats in the U.S.

As Prairie Business readers



know, attacks are happening in the United States as well. A recent example is the massive Marriott data breach, which exposed personal information of about 400 million guests.

Schools and hospitals are potential victims of cyber attacks, and financial institutions run into losses by means of counterfeiting and fraudulent money transfer.

To improve cybersecurity in this country, the U.S. International Strategy for Cyberspace has been officially recognized. National governance roadmaps for cybersecurity are provided by the National Institute of Standards and Technology. The National Checklist Program for IT Products, as spelled out by the NIST Special Publication 800-70, serves as the U.S. government's repository of publicly available security benchmarks. It offers detailed, low-level guidance on setting the security configuration of operating systems and applications used by various businesses.

Proactive efforts will help global CS

One must be living under a rock not to be struck by a sense of urgency and action in regard to CS, so I believe readiness should be premeditated and not an afterthought. With proactive policies, businesses and organizations can react when they are – not if they are – compromised.

To quote Kevin Streff, founder of SBS CyberSecurity and professor of information assurance at Dakota State University, when it comes to CS awareness and mitigation, businesses around the world need to stop kicking the can. They need to stop putting off cyber risk mitigation and

establish best practices such as compliance to Payment Card Industry Data Security Standard guidelines and requirements.

This is true in the U.S., in Ghana, and in every other country around the world.

Cybersecurity professionals can be proactive on a personal level as well, taking it upon themselves to find out what's going on outside their own country. They can do this by attending CS conferences to learn about best practices around the world.

As a future cybersecurity professional, I want to be part of the solution, so I am working to gain a comprehensive knowledge and understanding of the latest techniques in specialized information systems and cyber defense.

I can share this with my colleagues here or in Ghana, acting as a bridge of knowledge exchange.

My ultimate goal is to become a digital forensic or security expert/researcher working in a federal organization so that I may give back to society, helping citizens of all countries use technology to the best of their ability.

Francisca Afua Opoku-Boateng was born and raised in Ghana and completed her bachelor's degree in information technology at Valley View University there. She also has a master's degree in computer science and information systems from the University of Michigan.

She is a doctoral student at Dakota State University in Madison, S.D., working toward a degree in information systems with a specialization in cyber defense. She is expected to graduate in 2022.



It's tax time, avoid being scammed

We often put off doing our taxes until the last minute. But there's one very good reason to file well before April 15 – it's your best defense against tax-related identity theft.

Tax ID scams usually work like this: Someone who has obtained personal information such as your Social Security number and date of birth files a tax return in your name. They do so as early as possible, because the scam relies on the phony return getting to the Internal Revenue Service ahead of the real one. By the time you file, the scammer may have already gotten a refund, and you won't know you've been victimized until you get word from the IRS that it already has received your return.

Your tax data can be stolen in a number of ways: theft of mail or tax returns, phishing emails from impostors, or hacks of tax firms and employers' personnel records. Some tax scammers file in the name of deceased taxpayers, or steal children's identities to claim them as dependents.

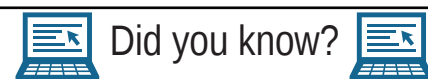
A joint crackdown by the IRS, state tax agencies and the tax-

AARP
Fraud Watch Network

preparation industry appears to be bearing fruit, with the IRS recording big declines since 2015 in the number of reported and confirmed cases of phony returns. But the fraudsters are fighting back, developing new ways to use your tax info to enrich themselves.

As with identity theft scams generally, it pays to be proactive in safeguarding personal data. But if you are victimized by tax ID fraud, call the IRS Identity Protection Specialized Unit at 800-908-4490 and notify your state tax agency.

For information about other scams, sign up for the Fraud Watch Network at www.aarp.org/fraudwatchnetwork. You'll receive free email alerts with tips and resources to help you spot and avoid identity theft and fraud.



Web browsing is customized for many users. Location-based services and targeted advertising is based on users' browsing history and other data collected and stored through cookies and third-party resources.

Consumers who are concerned about privacy or just want to have a better handle on what information they are presented have options. In addition to adjusting their browser history and cookie settings, individuals can rely on the Digital Advertising Alliance Self-Regulatory Program.

The DAA establishes and enforces responsible privacy practices across the industry for relevant digital advertising. The DAA offers consumers more transparency and control. Interested parties can visit <http://optout.aboutads.info/#/> and customize their browsing ad experiences - helping to increase or limit ads from certain sources.



Student cyber security precautions

Thanks to advancements in technology, students and educators are increasingly turning to birth, tablets and computers when working on daily assignments and classroom activities. Students rely on the internet for research and keeping in touch with teachers and other students, and work is even assigned and completed via digital platforms.

Despite the upside of technology, cyber crime is a potential pitfall of all that time spent online. The internet provides instant access, and that can put students at risk.

According to Verizon's 2016 Data Breach Investigations Report, the education sector ranked sixth in the United States for the total number of reported "security incidents." Schools are data-rich, meaning they give hackers access to information like identification numbers, birthdates, email addresses, financial data, medical records, and more.

Students must understand cyber security risks when working and sharing data online. The following are some tips students can follow.

- **Protect passwords.** Students are urged to keep their passwords to themselves. This prevents others from using accounts maliciously or even in seemingly harmless ways that can put you in trouble, such as searching for inappropriate content in school. Choose complicated passwords that can't be easily guessed, and opt for two-step authentication whenever offered.

- **Use secured WiFi networks.** Free or open WiFi connections are not encrypted, meaning they can be accessed by anyone. Many cyber crimi-

nals gain access to information through these channels. Schools should have encrypted systems in place.

- **Limit what you share on the internet.** Students are urged to be aware of what they share online. According to Data-Management, a computing service, information posted to social media is permanent, and deleted items aren't necessarily gone. Exercise caution on social media. Don't post unless it is something you would be comfortable sharing in public.

- **Watch out for phishing scams.** Phishing usually occurs through fraudulent email messages that mimic the look of reputable solicitations. Scammers rely on these tactics to tempt people to click on links or download attachments that can put malware on a device and steal personal data. Exercise caution with all links and downloads.

- **Schedule routine backups.** Data can be lost if a device crashes, so routinely back up personal devices and home computers. Backups can be stored on external hard drives or with cloud services.

- **Exercise caution when filesharing.** UC Santa Cruz's information technology services says viruses and malware can be transmitted by filesharing software, and files offered by others may not be what they say they are. Only use school-approved filesharing options.

Cyber security is something students should prioritize this school year. The right security measures can protect students, their classmates and their schools.

Riverdale native passionate about cybersecurity

By Daniel Arens

North Dakota recently saw one of its residents receive the first graduate cybersecurity credential in the state.

Ben Bernard, a computer service specialist and landscape architecture instructor at North Dakota State University, completed his graduate course in cybersecurity this fall at the school where he teaches.

"How do you figure out if you could do something?" Bernard said. "Well, you take one class and see how it works out, and go from there."

Bernard, who was born and spent part of his childhood in Riverdale, said he has always been interested in computer information systems. But the ever-expanding field of cybersecurity, and the need to protect businesses and individuals from the threat of hackers, opened a whole new world of possibility for him.

"I feel every IT [information technician] needs more security awareness, because of the evolving threat," he said.

Bernard's biggest passion, however, is in spreading the knowledge and enthusiasm he has for this field to other students. He developed a learning tool for students studying windows cybersecurity, and has been active in NDSU's Cybersecurity Student Association.

When Ben heard about the cybersecurity certificate, he got really excited, said NDSU assistant professor Jeremy Straub, who leads up NDSU's cybersecurity curriculum development efforts. While in the program, Ben has been its leading ambassador. There are people all over the campus and state that know

about the certificate program because of Ben.

Bernard received his bachelor's degree at Valley City State University in the late 1990s. He said people came to him looking for help with computer issues, which inspired him to pursue computer science and programming as a major.

After getting involved with NDSU, Bernard was quick to jump at the opportunity the cybersecurity credential provided to expand his knowledge and skills. He said one of the things that stands out to him most is the need to continue to update those knowledge and skills, and be ready for the unexpected.

"It's really important to learn how to learn, cause the job you end up holding might not exist right now."

- Ben Bernard

"It's really important to learn how to learn, cause the job you end up holding might not exist right now," Bernard said.

Bernard explained that there are certain courses related to different aspects of the cybersecurity field. He took classes on ethical hacking, forensics, windows security and cyber-physical system cybersecurity to earn his certificate.

Bernard had the opportunity to learn more about forensics, a field that fascinated him, from guest lecturers. He said that, beside what he learned about cybersecurity, this information has also helped him better address the regular day-by-day issues he encounters working as an IT.

There were other classes that caught his enthusiasm as well.

"A really amazing class was what we called certified ethical hacking," Bernard said. As the name implies, this course teaches students how to do hacking and penetrate secure systems. By learning how hackers operate, they are better equipped to help businesses address weak points in their own security.

Bernard isn't sure where the road he has now embarked on will ultimately lead. For the time, however, working with students is his passion.

"Tentatively, I'm really interested in cybersecurity education," he said. "There's so many opportunities, so not quite sure what the future would hold."

Bernard hopes to develop his own skills and help lead others to better assist the needs and concerns of a changing world.

"It's heartbreaking when you hear stories about people taken with a robo call or a spam," he said. "The bad guys get better, and so you have to stay on top of your game."

Bernard lived in Riverdale until he was 6 years old. His father was the manager at the Garrison Dam National Fish Hatchery at the time, and the family actually lived beneath the dam itself.

"I remember having a contest with my mom on who would be the first to reach that checkered red and white water tower," Bernard recalled. "I miss that beautiful water valley."

He added he still tried to get back that way every now and again when he's in the area.

"I love North Dakota, I'm raising two kids here," he said. "I'd love to see where I would continue to stay in the state and put my skills to work for the state."

April Showers of Savings

<p>25% off Office supplies, excluding ink cartridges & copy paper</p>	<p>25% off Coloring books</p>
<p>Paper 8.5x11 copy paper \$3.95</p>	<p>Elmers Glue: .75¢ for a 4 oz</p>

50% off
Little black & Little
pink address book

92 N Main St • Garrison, ND
701-463-2201

*Mention this offer. Limit one offer per purchase.
Some exclusions apply. Expires April 30, 2019*

Protect Your Identity

We Offer Cyber Security Insurance for Small Businesses and Identity Theft Protection for individuals in event of security breach.

Four locations to better serve you. Stop in for quotes and information today!

Security First Agency
OF NORTH DAKOTA

Center • 794-8759
New Salem • 843-7524
Mandan • 667-9000
Bismarck • 250-9001

Protect your smartphone from being hacked

For many smartphone users, their smartphones are never too far out of reach. It is a reflection of the role these devices now play in everyday life as well as the amount of sensitive information contained within them.

The treasure trove of personal information, including banking info, personal emails and private photos, that smartphones contain makes them tempting targets for skilled cyber criminals. Though phones come with built-in security features, savvy smartphone users recognize the importance of going beyond such features to protect their devices from hackers.

• **Update your operating system.** It can be a nuisance to update a phone's operating system. In fact, many a smartphone user has bemoaned an OS update, feeling the updates changed the look and performance of apps they had grown accustomed to. However, updated operating systems are offered for various reasons, one of which is to guard against glitches or bugs in old operating systems that might have made phones more vulnerable to hackers. When prompted to update a smartphone's operating system, do so right away.

• **Avoid public WiFi.** Hackers target victims in many ways, including through public WiFi hotspots. Smartphone users who don't have unlimited data plans may be tempted to use public WiFi when out and about. But doing so makes users vulnerable to skilled hackers who are just waiting to access unknowing users'

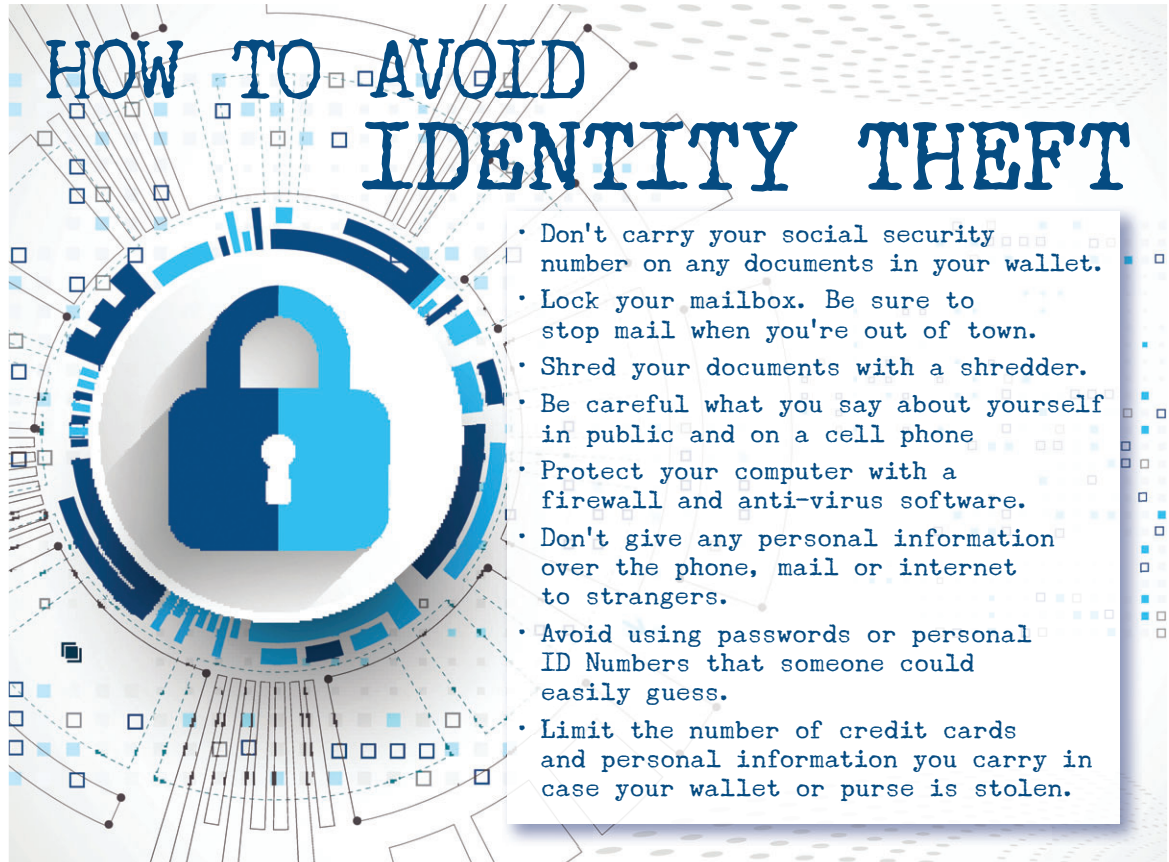
personal information, including their financial data. When leaving the house, turn off the WiFi on your phone, only turning it back on when you need it and only if you can access a secure network.

• **Accept two-factor authentication.** Two-factor authentication was designed so internet users would have another layer of protection against hackers. When attempting to sign into an account, whether it's email, social media, banking, or another login that requires a username and password, you may be asked if you want to enroll in two-factor authentication. This refers to the system in which users receive a temporary code via the messaging apps on their phones that only the users have access to. Some might say two-factor authentication is a nuisance, but receiving and typing in the short code will only take an extra few seconds and it's a great extra measure of protection against hackers.

• **Only buy apps from your phone's official app store.** When purchasing and downloading apps, only use official app stores such as the Apple Store or Google Play. Some hackers access phones via apps they offer through websites that, on the surface, seem legitimate. However, such apps contain viruses and malware that make it easy for hackers to access phones once they've been installed.

Smartphone users must recognize the importance of protecting their phones, and all the sensitive information their phones contain, from hackers.

HOW TO AVOID IDENTITY THEFT



- Don't carry your social security number on any documents in your wallet.
- Lock your mailbox. Be sure to stop mail when you're out of town.
- Shred your documents with a shredder.
- Be careful what you say about yourself in public and on a cell phone
- Protect your computer with a firewall and anti-virus software.
- Don't give any personal information over the phone, mail or internet to strangers.
- Avoid using passwords or personal ID Numbers that someone could easily guess.
- Limit the number of credit cards and personal information you carry in case your wallet or purse is stolen.



Farmers Security Bank

Community Banking At Its Best

Celebrating our first 100 years of serving you! 1919-2019



Washburn • 701-462-3232 • fsbwashburn.bank



Scammers are working hard to cheat you

Your local Beulah Police Department is working harder to be there for you and protect you!

IRS Scam

This scam is solicited over the telephone and the caller claims to be a representative of the IRS.

The Arrest Scam

The caller will claim that they are someone from the police department and that you, the citizen, have an active arrest warrant. If the citizen were to send money to them, then their arrest warrant would be cleared.

The Bond Scam

The caller will claim that someone close to them, family member or friend, has been arrested and you have to post their bond or they are going to prison.

The Foreign Scam

When family members are out of the country this may result in scamming calls. The caller will state that your family member or friend is sick, lost their wallet or need money.

The Unknown Debt Scam

This call revolves around the fact you, "haven't paid your bill." However, the caller is saying that it will result in reporting it to the Credit Card Bureau and they will come arrest you.

How to protect yourself

- Don't give personal information on social media
- Be familiar with the people that call you
- Don't open suspicious text
- Don't respond to phone calls about your computer asking for remote access – hang up – even if they mention Keep your personal details secure.
- Keep your mobile devices and computers secure.
- Choose your passwords carefully.
- Be wary of unusual payment requests and methods.
- Watch out for offers that seem too good to be true.



You just need to call 873-5252 or 745-3333 and assistance will be available to you

100% Wi-Fi

Double GIG | Faster Fiber | Stream TV | Security

STREAM ON!

Power your streaming device (Roku/Firestick) with the USB port on your TV. When you power off/on your TV it will do the same for your streaming device. This also makes it easy to reboot the device if it is in a hard to reach to location, such as a TV mounted on the wall. ~ Jody



USE MOUSE - TO RUN OR ASK

The 1st mouse had only one button & got the "click" name from the noise it made when pressed. It has evolved to two buttons - the left one & the right one. The easiest way to think of which one to use is: LEFT CLICK will do a command (run a program), RIGHT CLICK will ask a question (usually a menu of options). ~Riley



DON'T CLICK -

If in doubt or questioning if an email, link, or attachment is legit or safe - CALL WRT! ~ Stacy



EASY ON THE EYES

If you are having problems with text being too small when reading a webpage, the keyboard shortcut **CTRL + ENLARGES** the text. If you accidentally make the text to big, **CTRL -** will SHRINK the text back down. ~ Josh



BANDWIDTH BANDITS

Just because you aren't using the device doesn't mean its not doing anything. A lot of devices do updates when they are "sleeping" & use up your bandwidth depending on what they are doing. ~ Aaron



SIMPLE SEARCHES

Search right from the browser's address bar when online, there is no need to go to google.com or bing.com. Just type your search into the address bar at the top of the screen and hit enter, it will take you to a search results page related to your question. ~ Stephen



RESTART

When your device (smartphone, laptop, tablet) is acting up or not working right, restart the device. ~Kelsey



BE SAFE - BACKUP

Always backup your most important files and photos. Whether it is to an external hard drive, flash drive, or a cloud-based service (such as Google Drive or Dropbox) can be the difference between catastrophe and minor inconvenience if something were to happen to your device. Having your important files backed up to two different locations is even better, such as on a flash drive and Google Drive. ~ Tyson



www.westriv.com

TECH TIPS
from WRT Technical Support



Call Us @ 748-2211 • 24 Hour Tech Support To Help You!