OCTOBER
Issue 10

UNION BANK

Member FDIC
EQUAL HOUSING LENDER

Middlebourne Office
103 Dodd Street
Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street
Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street
St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy,
Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street
Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street
Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave.
Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street
Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2
New Martinsville, WV 26155
304-455-2967

BUSINESS CONTINUITY PLANS

We primarily think of these plans in the midst of a natural disaster and not necessarily a global pandemic. But here we are. The Coronavirus has affected every aspect of our lives. Businesses will now see how solid their plans are and if there are any gaps. If so, now is the time to fix them.

Business continuity planning is the process of creating systems of prevention and recovery to deal with potential threats to a company. The goal of these plans is to enable ongoing operations before, during and after a disaster. It helps determine an organization's ability to withstand severe changes in its environment and still be able to function. It also tests if an organization can adapt to changes temporarily or permanently that will help it successfully do business in a way that better suits their business needs. A good business continuity plan will include lots of bullet points but below are a few that contribute to the success of an organization's viability.

Technology Needs To Be Safe Guarded
When normal business flow is interrupted it can have a significant monetary impact. Having a solid Information Technology Plan is crucial to any business model. IT includes many components such as networks, servers, desktops, laptops and wireless devices.

The ability to run both office productivity and enterprise software is critical. All business continuity plans should include a component that has a strategy that addresses technology being restored to lessen down time.

Also, manual processes should also be a part of this strategy in the event computers are not readily available. The reality is your technology needs proper safeguarding and reliability to be able to recover quickly.

Protect Your Workforce
Organizations also need to ensure their workforce are protected. They should establish a strategy that enables employees to continue to function without endangering them. This would include but not limited to:

- Ensure employees can effectively work from home. (In other words, don't assume this to be the case. Test connectivity with multiple employees connecting at the same time to ensure that licensing and bandwidth won't be an issue).
- Verify that you have the tools, technology, capacity, and security measures in place to support a large remote workforce.
- Review your HR policies to ensure employees will not be personally impacted if they must be quarantined for an extended period and modify any policies as appropriate to give greater flexibility to normal working arrangements.
- Identify key employees and ensure other staff members have received appropriate training to comprehensively cover their absence. Now is the time for cross-training exercises to be completed!

Create a communications plan that includes providing employees and other stakeholders with regular situation updates as well as actions taken.

Information Security
It is not uncommon for criminals to prey upon victims during times of crisis. While your organization is swamped trying to bring order to chaos, criminals know that you have many irons in the fire and that's when they attack. Don't let your guard down! Proper information security processes are more critical during these times of upheaval!

Advise your employees to watch out for scams. There are many phishing emails making the rounds with startling Coronavirus details aimed at luring your employees to click on them. Warn your employees to avoid these traps!

Protect Your Customers and Their Information
Protecting your customers and their data is a crucial part of any business continuity plan. Data loss can have severe impacts that range from loss of revenue, compliance issues and reputational damage. Implementing strategies to reduce downtimes and having a data backup policy is a proactive way to minimize potential liabilities from the loss of critical customer data. It is always easier to recover from an emergency if your data is recovered.

The Coronavirus pandemic has proven to be a fluid situation that changes by the day. It is important to have a plan in place to deal with the business demands that are to come.

Sources:
https://www.ready.gov/business-continuity-plan
Business Continuity Plan | Ready.gov

https://www.saiglobal.com/hub/business-continuity-and-the-Coronavirus
https://www.hcamag.com/us/specialization/workplace-health-and-safety/coronavirus-hrs-role-in-business-continuity-plans/214862

7 BEST SOCIAL MEDIA PRACTICES

Social media platforms help us connect with friends and family, find jobs and share experiences. Social networks have become a powerful tool for everyone, but security is also an issue with these forms of communication. Hackers have found a way to exploit these methods of communicating, making it sometimes risky for people to share some of the best moments of their lives. Although social media provides great benefits, like with most things, there are also safety concerns.

Below is a list of 7 best social media practices that will help keep you safe while staying connected to friends and family.

1. Be careful of links you receive via direct message. Social media sites are a hotbed for phishing attacks. Although the link may seem legitimate, treat it the same way you would a treat a link you receive by email. If it looks suspicious, just delete it.

2. Don't divulge too much information. Yes, it is fun to post photos of recent trips or funny snip videos of your dog doing something crazy, but sometimes that is exactly the information a hacker needs to break into your accounts. Hackers usually go the route of "forgot your password" to try and steal information. The information you provide on social media may give them some hints on what your password could be just by scrolling through your timeline. As a precaution, you should never share what city and state you were born, home address, social security number, date of birth or any financial information.

3. Be selective of who you "friend" on a social media site. There are tons of fake profiles created by cybercriminals just so they can troll around and look for their next victim. This is an easy way to steal someone's identity.

4. Whatever you post will most likely be there forever. Think twice before posting something. Just because you delete it does not mean it's gone. The internet is very fast moving and whatever is posted can easily be printed and images and videos can be saved to computers for everyone to see, including future employers.

5. Do not allow social media networking services to scan your e-mail address book. Normally when you join a social media site they ask to scan your inbox so you can invite your contacts to "follow" or "friend" you. If you agree everyone in your contact folder will receive an email from that site.

6. Check your privacy settings. Many of the sites allow you to customize your settings to limit who and what groups can see various aspects of your personal information.

7. Educate, Educate, Educate. Kids love social media! Playing games and anything that looks intriguing to their eyes can potentially be very dangerous. Talk to your kids about avoiding clicking on links that promise great "prizes" or playing games that may post or share information without your knowledge. If it seems too good to be true, then it probably is. Many of these games and contest are a direct link to a phishing scam.

Sources:
http://seniornet.org/blog/11-tips-for-social-networking-safety/
http://www.networkworld.com/article/2346606/microsoft-subnet/12-tips-for-safe-social-networking.html