RELIABLE IT BANKING

THE VAULT

Reliable IT Referral Program

We appreciate the opportunity to serve you and your referrals are one of the highest compliments we could receive. When you refer someone to Reliable IT, you trust us to deliver superior levels of quality and service to a company you respect as well.

We value your trust, and as a way to thank you for your referrals, we offer this incentive to our clients:

Introduce us to a new prospective client and if that client signs an agreement for Managed Services, you will receive the amount of their first monthly fee (minus 3rd party costs) credited to your company's statement for Reliable IT services, up to one month of *FREE* services, on your next bill.

For More Information, please contact:

Aaron Biehl at 866.634.3230 or Abiehl@RITBanking.com

March 2020

This monthly publication provided courtesy of Aaron Biehl, Chief Operating Officer, Reliable IT Banking.

We are a 24-year-old SOC 2 Managed IT, Security and Compliance Provider for Community Banks Nationwide. We provide monthly support to 40+ Community Banks representing 4500+ devices under management. Our standard of excellence includes personalized attention with a dedicated team, 24/7 live answer/monitoring, & on-going innovative engagements with your key stakeholders to ensure IT is effective, secure, and accelerates growth.

5 Signs You're About To Get Hacked — And What You Can Do To Prevent It

Hackers love to go after small businesses. There are many businesses to choose from, and many don't invest in good IT security. Plus, many business owners and their employees have bad cyber security habits. They do things that increase their risk of a malware attack or a cyber-attack. Here are five bad habits that can lead to a hack and what you can do to reduce your risk.

1. Giving out your e-mail Just about every website wants your e-mail address. If you share it with a vendor or e-commerce site, it's usually not a big deal (though it varies by site – some are more than happy to sell your e-mail to advertisers). The point is that when you share your e-mail, you have no idea where it will end up – including in the hands of hackers and scammers. The more often you share your e-mail, the more you're at risk and liable to start getting suspicious e-mails in your inbox.

If you don't recognize the sender, then don't click it. Even if you do recognize the sender but aren't expecting anything from them and do click it, then DO NOT click links or attachments. There's always a chance it's malware. If you still aren't sure, confirm with the sender over the phone or in person before clicking anything.

2. Not deleting cookies Cookies are digital trackers. They are used to save website settings and to track your behavior. For example, if you click a product, cookies are logged in your browser and shared with ad networks. This allows for targeted advertising.

Continued on pg.2

There's no good way to tell who is tracking online. But you can use more secure web browsers, like Firefox and Safari. These browsers make it easy to control who is tracking you.

In Firefox, for example, click the three lines in the upper right corner, go into the Options menu and set your Privacy & Security preferences. Plus, every web browser has the option to delete cookies – which you should do constantly. In Chrome, simply click History, then choose "Clear Browsing Data." Done. You can also use ad-blocking extensions, like uBlock Origin, for a safe web-browsing experience.

3. Not checking for HTTPS Most of us know HTTP – Hypertext Transfer Protocol. It's a part of every web address. However, most websites now use HTTPS, with the S meaning "secure." Most browsers now automatically open HTTPS websites, giving you a more secure connection, but not all sites use it.

If you visit an unsecured HTTP website, any data you share with that site, including date of birth or financial information, is not secure. You don't know if your private data will end up in the hands of a third party, whether that be an advertiser (most common) or a hacker. Always look in the address bar of every site you visit. Look for the padlock icon. If the padlock is closed or green, you're secure. If it's open or red, you're not secure. You should immediately leave any website that isn't secure.

4. Saving passwords in your web browser Browsers can save passwords at the click of a button. Makes things easy, right? Unfortunately, this method of saving passwords is not the most secure. If a hacker gets your saved passwords, they have everything they could ever want. Most web browsers require a password or PIN to see saved passwords, but a skilled hacker can force their way past this if given the chance.

Protect yourself with a dedicated password manager! These apps keep passwords in one place and come with serious security. Password managers can also suggest new passwords when it's time to update old passwords (and they remind you to change your passwords!). LastPass, 1Password and Keeper Security Password Manager are good options. Find one that suits your needs and the needs of your business.

5. You believe it will never happen to you This is the worst mentality to have when it comes to cyber security. It means you aren't prepared for what can happen. Business owners who think hackers won't target them are MORE likely to get hit with a data breach or malware attack. If they think they are in the clear, they are less likely to invest in good security and education for their employees.

The best thing you can do is accept that you are at risk. All small businesses are at risk. But you can lower your risk by investing in good network security, backing up all your data to a secure cloud network, using strong passwords, educating your team about cyberthreats and working with a dedicated IT company. Good IT security can be the best investment you make for the future of your business.

> **"Good IT security can be the best investment you can make for the future of your business."**

7 Things To Do So You DON'T Get Hacked When Shopping Online

1. Verify the URL is safe. Many browsers have a little padlock in the URL bar. If the padlock is closed, the URL is safe. If it's open, you may want to avoid the site.

2. Verify the URL is accurate. Many scammers register fake websites using misspelled URLs or extra numbers to look like the real deal. If the URL looks odd, it's probably a scam.

3. Use a secure web browser. Firefox and Chrome, for example, always navigate to HTTPS (Hypertext Transfer Protocol Secure) websites. These websites are more secure than their HTTP counterparts.

4. Don't click suspicious links or attachments. Never click a link if you can't verify it first. In fact, it's better to delete any e-mail you don't recognize.

5. Always bookmark authentic websites. When you bookmark real websites, you never have to worry about mistyping or clicking scam links.

6. Rely on a password manager. It's hard to remember strong passwords, but with a password manager, you don't have to. Never use a bad password again!

7. Use the official mobile apps for online stores. If you download the official app of your favorite online stores, such as Amazon or eBay, you don't have to worry about accidentally navigating to a scam website. Just make sure the app is verified by Google or Apple.

Lifehacker, Nov. 19, 2019.

Place Your Bet

with Reliable IT Banking!

Don't Gamble with your IT!

Complete your FREE IT and Compliance Assessment

To determine your bank's:

1. IT Infrastructure
2. Cybersecurity
3. Business Strategy
4. Disaster Planning
5. Software & Compliance

To complete your assessment, visit:
www.RITBanking.com/free-it-and-compliance-assessment/
Or contact:
Aaron Biehl at 866.634.3230
ABiehl@RITBanking.com

Don't Gamble with Your IT... Place your Bet with Reliable IT!

RELIABLE IT
BANKING

1540 Main St.
Suite 218, #107
Windsor, CO 80550

Inside This Issue:

To view previous newsletters, visit: **www.RITBanking.com/about/newsletter/**