# BANKING DATA SECURITY CHECKLIST

## 20 Ways to Keep Hackers Out and Protect Your Bank


309.664.8150 sales@integrityts.com integrityts.com

INTEGRITY TECHNOLOGY SOLUTIONS

**Data Security** should sit firmly at the top of the priority list for every bank. As technology needs increase, so do threats to the sensitive data that banks need to protect. Financial institutions have the added burden of meeting regulatory standards and compliance requirements.

Your bank is entrusted with protecting the sensitive personal data of your customers. That responsibility looms large and should be priority one.

On the next page, test your bank. Using the checklist, mark the items that are currently included in your comprehensive data security strategy. Seeing several unchecked boxes at the end? It's time to revisit your strategy to ensure that your bank is safe from hackers and other threats.

### 1. Always use unique and complex passwords

Using a Password Manager can help generate and keep track of credentials. Just be sure that your Master Password can't be guessed. Passphrases will minimize the likelihood your accounts can be accessed. Be sure you have policies in place to change passwords and passphrases multiple times per year. ☐

### 2. Encrypt everything

Hackers and cyber criminals continue to become more creative in stealing data. Using encryption can help foil their plans. ☐

### 3. Monitor your Network for suspicious or unauthorized activity

Hackers are vigilant, so businesses need to be too. Actively monitoring your network can help catch hackers before they walk away with sensitive data or hold your data hostage. ☐

### 4. Protect remote access

Accessing important business data should only happen in controlled environments, ideally. If there are exceptions, make them few and far between and have a plan if things go wrong. ☐

### 5. Test for system vulnerabilities

What you don't know can hurt you when it comes to data security. Even if you feel that your data is safe – test it. Try to get past your own defenses. If vulnerabilities exist, be the one to find them. ☐

### 6. Update all software as soon as it's made available

Software updates may seem like a pestering nuisance of computing, but they often contain security patches. Keeping your network up to date can be critical in preventing attacks. ☐

### 7. Backup and conduct restore testing of your data regularly

Backing up data is an important facet of any security strategy. In the event of a cyber attack, a natural disaster or other large-scale emergency, having a backup policy in place can save and restore data. ☐

### 8. Have a cyber security response procedure in place

When your business suffers an attack or is compromized, time is of the essence. Know who will be involved in the process and what steps to take to safely restore your network and data assets. ☐

### 9. Have a plan for Cloud Security

The Cloud gives businesses enormous storage capabilities without the logistics and cost attached to prior methods. But, the Cloud requires diligent data security measures. Before storing important data in The Cloud, find out how to keep it safe. ☐

### 10. Implement multi-layered security

Using a multiple step verification process and other multi-layered security measures makes your business a less appealing target and slows hackers down. ☐

### 11. Be wary of sharing your mobile device

Smartphones, tablets, and more can give cyber criminals access to business data. Use a password-protected lock screen and other features to ward off hackers. In general, be wary of who is using your mobile device. ☐

### 12. Educate your staff about data security threats

One of the best ways to prevent a data security issue is training your staff to be prepared for it. Review best practices, policies, and standards for protecting your business. Communicate the current threat landscape and how to report suspicious activity ☐

### 13. Avoid e-mailing sensitive information

E-mail is a vulnerable communication method that can easily be accessed. If employees are discussing or sharing sensitive data over e-mail, they're putting the company at risk. Encrypted email can mitigate this risk. ☐

### 14. Install and update malware, spyware, and ransomware defense software

Having preventative antivirus software on your network computers can help detect and combat common hacking tools. ☐

### 15. Stay up to date on browser updates

Browser updates often strengthen the security of that browser. The more secure the browser, the more secure your data will be. ☐

### 16. Develop a Social Media policy

Social media is a highly visible and easy platform on which to jeopardize company data. Train employees to be careful with their activity and what they're sharing where. ☐

### 17. Control access to computers, devices

Develop and maintain a standard for granting access to sensitive data. Keep authentication standards high and keep data hidden as much as possible. ☐

### 18. Be mindful of physical data

If there are physical copies of sensitive data created, know where those copies are and where they'll end up. ☐

### 19. Use the lowest role possible to access what you need

If you can access what you need without using an Administrator log in, do that. Use Admin only in cases where it's absolutely necessary – there's no reason to open data up to threats needlessly. ☐

### 20. Secure your Wi-Fi network

Don't let hackers intercept data or compromise your network through your Wi-Fi connection. Secure it with a strong password. ☐

Does your business need help with an updated security strategy?

Integrity Technology Solutions is a local IT security and support provider for businesses in central Illinois. We specialize in compliance, data security, security awareness, disaster recovery and IT support.

Integrity will stay on top of the latest and greatest security measures for your business, offering multiple layers of protection for your data assets. We offer best in class services related to detecting malicious activity, and we provide structured cyber security triage response services. Integrity also incorporates a security awareness program that will help your staff to become “protectors of information”.

Integrity can help your business make the right decisions related to your security strategy while eliminating wasteful spending.

Contact Integrity today for a free IT security needs analysis.

## *INTEGRITY IS A PROMISE IN ITSELF: INTEGRITY WILL ALWAYS ACT IN YOUR BEST INTEREST.*

If your business needs a better approach to IT, Integrity can be reached at (309) 664-8150.