CHECKLIST

Machias
Savings Bank

Cyber security checklist

Cyber security is a constantly changing threat landscape that can leave your organization vulnerable. These measures can help protect your organization.

Back up your data

- □ Backup data from customers or staff
- □ Backup data, documentation and manuals
- □ Backup system configurations and log files
- □ Set backups to happen automatically
- □ Run backups regularly
- □ Store your backups in an accessible safe location

Use up-to-date systems

- □ All devices are supported by manufacturers
- □ System updates installed automatically
- □ IT provider applies updates within weeks of release
- □ Software used on network is supported

Control access to data

- □ Only store necessary information from customers
- □ Encrypt any data in transit (e.g., using HTTPS)
- □ Encrypt any data at rest (e.g., in a database)
- □ Employees only have access to necessary data
- □ Staff cannot access network with insecure apps

Enforce password security

- □ Strong password policy for access to your systems
- □ Choose a MFA solution for the company
- □ Setup applications to enforce MFA on logins
- □ Set-up each employee with MFA access

Secure your email

- □ Set up email monitoring
- □ Review DNS settings for each email service and update

Secure your cloud services

- □ Cloud services are backing up your data
- □ Setup 2FA by default
- □ Opt-in to notifications of security breaches

Monitor activity

- □ Log failed login attempts
- □ Log password changes
- □ Monitor anti-malware notifications
- □ Clear point of escalation for suspicious transactions

Write a security policy

- □ Create a security policy document
- □ Plan for responding to a cyber security attack
- □ Include password and data policy

Onboarding and exit processes

- □ Add security training to employee on-boarding
- □ Educate staff about the security policy
- □ Systemize removal of access when employees leave
- □ Record items to be returned when employees leave
- □ Set up exit interviews when staff leave

Machias
Savings Bank

Cyber security checklist

Back up your data

It's essential you have a system for your backups and regularly test them. Decide if you'll use cloud-based or on-premise backups and data storage. The frequency of backup you choose would depend on your business (for example if you do many transactions every hour, you may need to back up in real time, but if you only have a few changes each day, then a daily backup may be ok.) Backup systems should be automated and well protected with passwords and MFA. If you have physical backups make sure that you keep a copy off site in case of a fire or natural disaster.

Use up-to-date systems

Reduce system vulnerabilities by keeping all your devices and software up-to-date.

Verify that all servers, computers, and mobile devices are supported by the manufacturer to receive updates. (and preferably to run updates automatically) and inform staff to do the same.

For BYOD devices such as personal laptops and phones, ensure they run supported systems and software before accessing the business network and keep them updated.

Control access to data

Protecting your systems (computers and networks) is crucial to protect your business and customers' information. Restrict who is allowed access to your systems and where possible, use access privilege settings on hardware and software (for example, administrator, operator, editor, etc). Consider locking cabinets, password protecting computers and installing security cameras. Anti-virus and firewall software should be installed to protect against cyber threats.

Make sure your networks are secured with complex passwords to prevent anyone hacking in from outside your business. If you offer wifi access for your customers, this should be on a separate network to your internal systems.

Enforce password security

You need a password policy for accessing company systems. For example, require passwords that include letters, numbers, symbols, case sensitivity and length. You could include a policy on how often passwords must be changed. This can often be enforced using software settings.

Multi-Factor Authentication (MFA)

Multi-factor Authentication (MFA) is an authentication method that requires users to provide additional credentials to gain access to an application, online account, or a network. It usually involves a special code being sent to the user's phone either via text message or an application on their phone.

Record how you will use MFA in your business. Adding Multi-Factor Authentication to your accounts helps protect against many of the biggest threats to your data such as phishing attacks, brute-force attacks and password reuse.

Secure your email

Lock your email so only authenticated users can send emails from your domain. Email can be hacked to send spam that appears like emails sent from your email accounts. Using spam filters, quarantines and the correct SPF, DKIM and DMARC records in your domain setup can all help secure your email. If you use third-party services for email (for example, email newsletters, forms on your website, etc.) then adding these records can also improve deliverability.

These records can be found in your domain settings. If you cannot do this yourself, consult a domain expert to check these for you.

Consider using an email monitoring service that can check if your emails are being delivered and whether anyone is trying to use your email address to send phishing emails.

Cyber security checklist

Secure your cloud services

Cloud services offer benefits like software access on a month-by-month basis (Software as a Service or 'SaaS'), data accessibility from any device, and storage with backups.

Before committing, check the documentation and small print for information about data backups, two-factor authentication, security breach notifications, data handling if the company changes ownership, and their public security policy. Ensure they have a way to report security issues, as the absence of this can be a red flag.

When using cloud services, it's sometimes important to check the jurisdiction of the servers holding your data, as some of your customers may have policies on where their data can be stored.

Monitor activity

Logs can be vital when locating the source of a security breach and to alert you to potential or actual security incidents, such as multiple failed logins or logins from unknown IP addresses.

Early detection allows for quicker action to protect your business.

Consider monitoring logs for:

- Failed login attempts
- Successful logins to your CMS
- Password changes
- Denied 2FA requests
- Anti-malware notifications, and
- Network connections.

Your IT service provider can assist with this setup.

Look out for online fraud, such as invoice scams.

Manually verify new supplier payments or changes in bank details by phone or text before approving. This applies to any unusual or unexpected requests. For instance, if a supplier emails a request to change their bank account number, call them to confirm the email's authenticity.

- Establish a process for specific transactions, like phone verification for large orders or changes.
- Use a separate communication channel to verify transactions or changes, such as following up an email with a text or call.
- Create a clear escalation point for staff. Ensure they know how to handle suspicious emails, incorporating this into your incident response plan.

Write a security policy

Assign a person to manage your security policies. Document your requirements (like those in this plan) that you need to keep your information and employees safe. Test and implement.

Setup onboarding and exit processes

Cyber security breaches usually begin by errors made by people within the business. Your employees should know your security policies and why they exist. Store policies in a central place that is accessible to all employees.

Cyber security checklist

Notes

Note
This is a guide only and should neither replace competent advice, nor be taken or relied upon as financial or professional advice. Seek professional advice before making any decision that could affect your business.