Cybersecurity Resource Kit

Protect Against Cyberattacks • **Computer Usage** • **Identifying Phishing Emails** • **Information Security**

G&A Partners

Time to grow.

gnapartners.com

Protecting Your Small or Mid-Sized Business Against Cyberattacks

If you think cybersecurity is something only large companies need to worry about, think again.

The 2022 Data Breach Investigations report by Verizon found that 61% of small businesses were targeted by cyberattacks in 2021. But, shockingly, a 2022 survey published by Digital.com shows that 51% of small businesses don't have a cybersecurity prevention plan.

Use these checklists to begin developing a prevention plan that will help you protect your business against cyberattacks.

HR Checklist

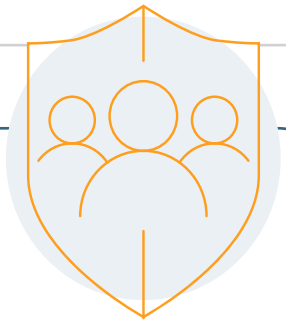
- [ ] Develop a team of IT and department leaders to discuss cybersecurity initiatives and ensure cybersecurity is viewed as a company-wide effort, rather than an effort solely driven by IT.
- [ ] Update IT regularly as employee roles change and their required access to data changes, ensuring employees only have access to data they need for their position.
- [ ] Draft and implement sound employee policies, including a computer/internet usage policy and an information security policy. Use our sample policies to get started.
- [ ] If you have remote/hybrid employees, create a remote/hybrid work policy that outlines cybersecurity expectations when employees are working outside of the office.
- [ ] Provide consequences that are flexible based on whether an employee's infractions are infrequent and require additional training or infractions are frequent and cause for more serious consequences.

Employee Education Checklist

- [ ] Develop an employee training program on company-specific policies and procedures, as well as general best practices for maintaining cybersecurity.
- [ ] Plan employee education throughout the year so employees view cybersecurity as an ongoing effort.
- [ ] Utilize a variety of training materials, such as online courses or our guide on phishing.
- [ ] Build in an evaluation method to test each employee's understanding of cybersecurity information and best practices, such as quizzes after an online course or simulated phishing attacks. Provide follow-up training for employees, if needed.
- [ ] Set deadlines for employees to complete training and hold them accountable when deadlines are missed.

Checklists - cont.

Protecting Your Small or Mid-Sized Business Against Cyberattacks



Note: If you work with a third-party vendor to manage your IT needs, use this checklist as a conversation-starter with your vendor.

IT Checklist

- [ ] Install, use, and regularly update antivirus and antispyware software on all computers.
- [ ] Download and install software updates for your operating systems and applications as they become available. If possible, choose the automatic update option.
- [ ] Regularly make backup copies of important business data.
- [ ] Control who can physically access company computers and other network components.
- [ ] Ensure that your business network is encrypted and do not allow unauthorized users to connect to it.
- [ ] Require individual user accounts for each employee rather than allowing employees to share accounts.
- [ ] Limit employee access to data/information and authority for software installation.
- [ ] Require all employees to use strong passwords or a secure password management application.
- [ ] Monitor, log, and analyze all attempted and successful attacks on systems and networks.

UP NEXT: Computer Usage

Computer Usage

Below is a sample computer/internet usage policy an employer might include in its employee handbook.

[Company name] provides computers and internet access to employees for business purposes. Employees must adhere to the following requirements when using company-provided computers and internet access:

- Company-owned devices (computers, tablets, cell phones, etc.) are for business use only.
- Employees accessing the internet via Company hardware/software are representing [company name]. As such, their conduct should be ethical and lawful at all times.
- Email, software, and other information systems that are provided by the Company to facilitate your ability to do your job efficiently and effectively are to be used solely for business purposes; incidental or personal use is prohibited unless authorized by your immediate supervisor or an officer of the Company.
- At any time the company may intercept, monitor, review, copy, and/or download any communication or file you create or maintain on these systems.
- When using the internet, employees should not send sensitive materials or those that constitute confidential Company information unless approved by an officer of the Company and the information is properly encrypted to prevent any interception by an outside party.
- Harassment of any kind is strictly prohibited. Messages with derogatory, or inflammatory remarks regarding race, religion, national origin, sex, or other protected classes may not be transmitted through Company systems.
- Employees may not download software without the express acknowledgment and approval of the Company's network administrator to ensure that proper licenses are obtained and viruses are not transmitted.

Your consent and compliance with this policy is a term and condition of your employment. Failure to abide by these conditions or to consent to any interception, monitoring, copying, reviewing, and downloading of any communications or files will result in disciplinary action, up to and incuding termination.

This sample policy is provided as an example only. This information is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.

UP NEXT: Identifying Phishing Emails

Tips for Recognizing a Phishing Email

What is phishing?

"Phishing" is the fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords, credit card numbers, etc.

Phishing emails, for instance, may look like they're from a sender you trust (like your bank, a social networking platform, or a retailer). If you respond to that email or click on links within the message and then provide your username, password, bank account information, credit card number, or other data, you may not realize you're being scammed until it's too late. With this information, a hacker can quickly take over your identity and steal from you or your business.

Phishing scams can also take place via phone and text. These attacks are known as vishing and smishing.

You might assume that phishing emails are obvious to spot, but they're getting more sophisticated by the day.

In many cases, attackers can nearly replicate a business' logo and letterhead, making it almost impossible to distinguish these fake emails from the real thing. But there are some telltale signs you can watch out for:

- Be cautious of ANY email you receive that contains links and attachments -- even if it's from someone in your contacts.
- Compare this address with any known emails you have from the actual sender. Many attackers will switch around a couple of letters so that the address looks legit at first glance.
- Hover your mouse over the link provided to see the actual URL. Like fake email addresses, fake web addresses may contain very subtle differences (like a single letter being out of place).
- Check the email text carefully, especially for proper spelling and grammar. Legitimate emails sent from well-known companies will usually not contain spelling or grammatical errors.
- Keep in mind that no legitimate company will send you an email asking for your personal or account information. A general sense of urgency (like warning that your account will expire if you fail to provide information) is something that should immediately raise suspicion.

Information Security

Below is a sample information security policy an employer might include in its employee handbook.

[Company name] takes data security very seriously. Each employee is responsible for assisting in supporting the Company's efforts to achieve its goals of safeguarding corporate and client/customer information.

Basic guidelines for securing sensitive information include:

- Computers/laptops are required to be locked when leaving your desk for any period of time.
- Documents that contain personal information must be securely locked away every night.
- Employees must collect/remove all paperwork from printers/copy/fax machines promptly.
- Disregarded paperwork must be shredded or placed in a secure shred bin. This includes, but is not limited to, sticky notes, handwritten messages, printed emails, etc.
- Stolen or misplaced equipment (laptops, mobile devices, access badges, etc.) must be reported to the Company IT staff immediately for deactivation and further investigation.
- Laptops must be securely locked away or taken home every night. Laptops should also never be left in plain sight inside of any vehicle.
- Emails containing confidential information sent to clients/customers should be sent via a secure portal.
- Files received have the potential to contain computer viruses. Employees should review all communication received to ensure it originates from a credible source before clicking on any links or opening any attachments.
- Employees should store all login information within a Company-approved secure password management application and should never share or divulge passwords.

Your consent and compliance with this policy is a term and condition of your employment. Failure to abide by these guidelines will result in disciplinary action, up to and including termination.

G&A Partners has got your back (office).

Sound employment policies can protect your business from vulnerabilities arising out of misunderstandings and mistakes that may lead to embarrassing errors, injuries, and expensive lawsuits and litigation. Learn how G&A Partners' HR experts can help protect your business at **www.gnapartners.com.**