mailprotector®

WHEN CYBER ATTACKS STRIKE

The ultimate MSP guide to preparing for cyber attacks

Section 1

BUILD YOUR OWN INCIDENT RESPONSE PLAN

If you don’t have one already, you need to create an incident response plan. Should a cyber attack occur, you need to be able to follow a plan that was laid out when your organization was not under duress. **Doing so will allow you or your clients to calmly open your plan and get to work.**

A solid incident response plan will help you think through all areas of your business – not just the technical side. To properly build an effective plan, you’ll need to be mindful of everyone who will both be impacted and involved with the security restoration process.

This section will walk you through considerations you should take in defending against attacks and building your own incident response plan.

CREATING YOUR PLAN

Here are things to consider when building an incident response plan. These are steps you will need to consider should a breach occur.

- **Document everything** and establish a place where you can securely store it for safekeeping.
- **Limit user access immediately** so only trusted users may access critical business systems.
- **Reset Access.** Once a cyber attack occurs, reset all access to critical systems.
- **Establish a plan for your help desk** to avoid creating a pseudo-DDoS attack. Determine how your help desk will mitigate the influx of calls and tickets.
- **Identify the "off switches"** for each of your business-critical systems. In case an attack occurs, you need to be able to calmly disable access.

- **Create alternative communication methods** so you'll still be able to communicate if IM or email is unavailable (in the event of a breach).
- **Establish or identify a communication channel** where you'll be giving your customers regular updates.
- **Familiarize yourself** with how to keep logs, do memory dumps, download network traffic reports, and save disk images. Before you pull the plug on systems, you are going to want this valuable information for digital forensics. But you don't want to spend unnecessary time trying to remember how to do this.
- **Establish a breach response team**. This team should consist of a group of people who actively meet periodically during the breach. You know your business best, but we recommend a blend of IT, legal, customer service, and communications professionals.
- **Reset passwords** for affected, and potentially affected users. Reset them again once the cyber attack remediation is complete.
- **Determine which systems are to be prioritized** for return to service. Typically, communication channels are high on the list because alternate communication channels may not be conducive to all customers. You may also want to use this time to keep a list of all systems and their respective owners.
- **Organize a list of contacts** for vendors' support teams. During an incident, you may need to contact vendors and inform them to carefully vet communication. Don't limit the vendors to your IT services. The customers' vendors may be at risk also.
- **Activate business continuity virtual instances.** If you have business continuity in place, determine if virtual instances can be brought online to restore essential business services. This can ease the stress and urgency during the remediation phase of a breach.
- **Contact the proper authorities**. Understand when and how to contact law enforcement or regulatory authorities. If a breach constitutes large financial losses, regulatory failures (HIPPA, FINRA, etc.), or blatant disregard for security protocols, you may need to involve other organizations.

Section 2

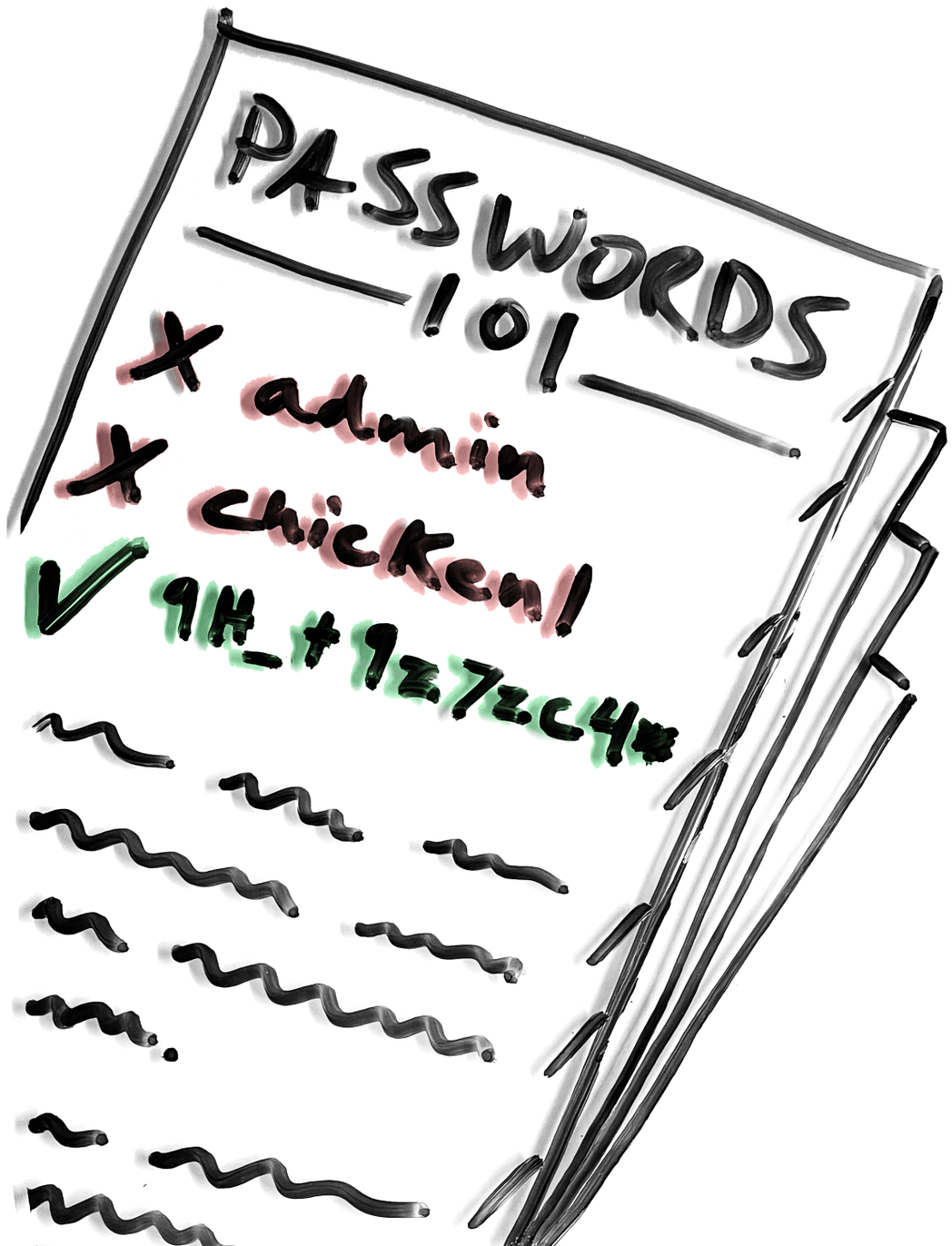
BE SMART AND DO YOUR BEST TO PREVENT A CYBER ATTACK

As the old adage says, **an ounce of prevention is worth a pound of cure**. This ring especially true for today's business users where one misinformed click could potentially create shockwaves of damage that are felt for years.

Hackers are organized, smart, and know how to exploit weaknesses in every imaginable aspect of an infrastructure. They also know what **mistakes are commonly made in the workplace** and where human beings tend to lower their guard, incorrectly assuming that they will be "safe enough".

Thankfully, there are many easy-to-implement precautions anyone can take to stay safe. Let's look at some things your organization can do to drastically **reduce your chances of being victimized** by an email-based attack.

WHAT YOU CAN DO



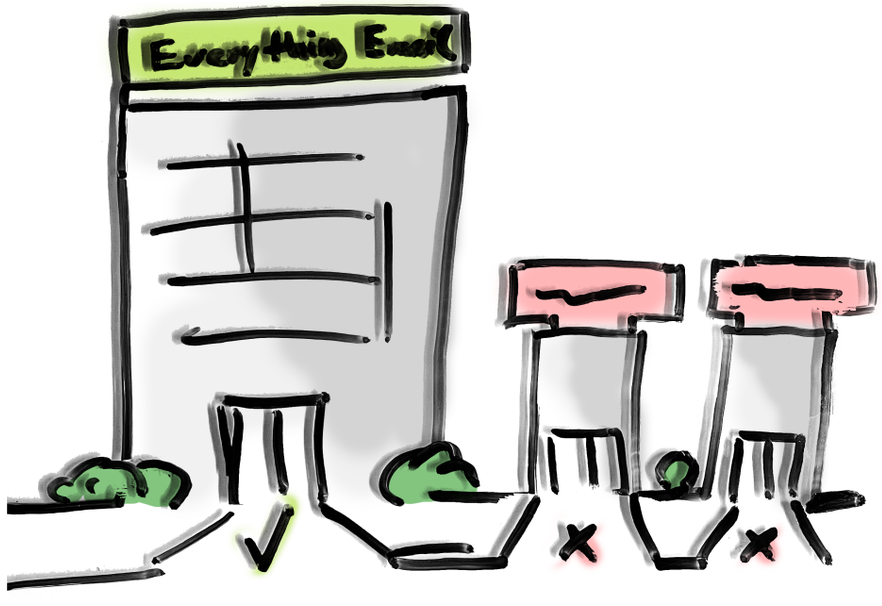
Here are a few proactive things you can do to defend your clients against cyber attacks, before a cyber attack occurs.

- **Implement MFA** where possible.
- **Use a password management tool** so you can control access in case a hack occurs. Tools like LastPass or 1Password will help.
- **Enforce hard-to-guess passwords** for all users. After the New Cooperative cyberattack audit, IT experts discovered a large percentage of users were using the password “chicken1.” Not the most brilliant idea when you consider the amount of poultry they produce.
- **Change passwords** for Wi-Fi and administrative tools regularly.
- **Monitor while you’re away**. Cyberattacks often occur on the weekends, giving threat actors more uninterrupted time to operate without detection.

- **Outsourcing or operating a SOC** (security operations center) can provide closer eye on IT operations 24x7.
- **Take advantage of alert capabilities**. Some vendors provide native alerting that can feed information to an RMM (remote monitoring & management) or ticketing system.
- **Add a secure smart host or relay** to the customers' outbound emails.
- **Invest in cloud-based endpoint protection** solutions and email security solutions so network changes can be made quickly in case of a potential breach.

Be smart! Alerts can keep a small problem from blowing up.

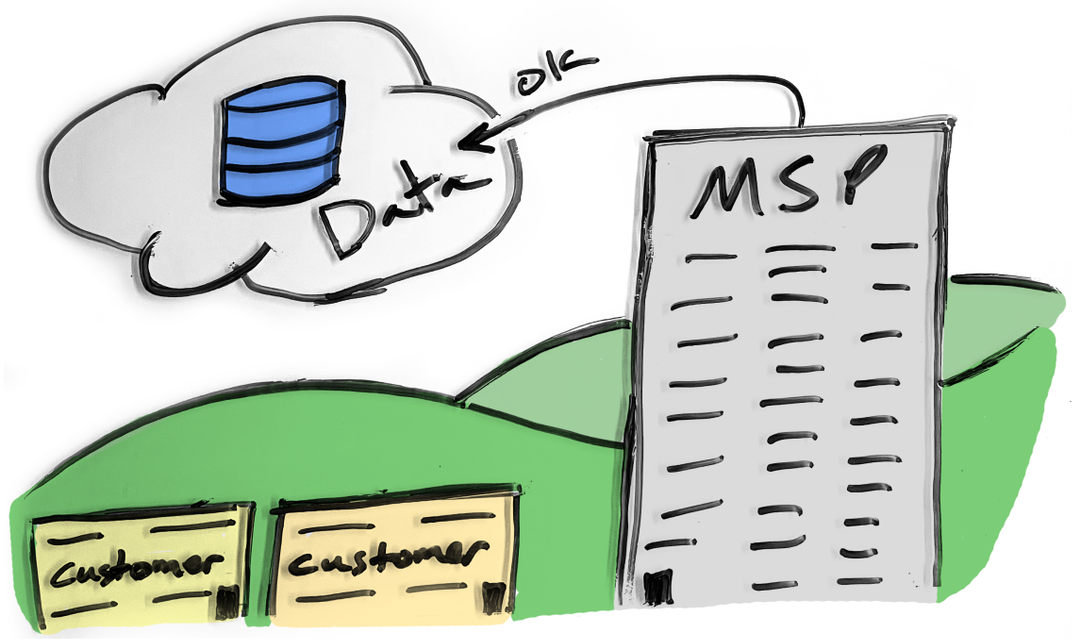
- **Install proactive network monitoring** for the most sensitive networks and data.
- **Choose the right vendors** and centralize as much as you can. This includes logs and network monitoring, but also minimizing the number of vendors whose software you're managing as part of your stack. Make sure you have a complete solution, but only take on what you can handle. The more niche pieces of software you have, the more potential gaps between systems there will be. Eliminate homegrown solutions wherever possible.



Choose one email security vendor that does everything you need.

- **Consider privileged access** management. If a breach occurs, make the privileged accounts available to technical teams so they can quickly access your core systems.
- **Keep all systems updated** with the latest versions.
- **Stay familiar with HIPAA and PHI requirements.** If you hold HIPAA data or PHI, you'll want to be familiar with the HIPAA Breach Notification Rule and take note of the breach notification requirements.
- **Secure remote machines**. With an increase in the mobile workforce, administrators must find ways to better secure machines outside of the network perimeter. So many attacks happen when company-owned computers go off-network.
- **Educate your user base** and keep threat awareness up, even if it requires spending money.
- **Eliminate unused elements** such as software, licenses, and email accounts.
- **Implement a complete email security solution** that includes a secure email gateway. Don't fall for the rhetoric from the vendors marketing an API solution without one. Secure email gateways allow you to have control over the entire email process, not just part of it. Read more about the benefits of a secure email gateways vs. an email security API.
- **Be sure your solution has all the essentials**: inbound filtering, outbound filtering, privacy and email encryption. These need to be found in a single solution, rather than piecemealing, which can leave vulnerabilities. Email is a very common medium through which cyberattacks occur. What Office 365 and Google Workspace offer are too fundamental, so each solution exposes its users to well-known vulnerabilities. Investing in a stronger, more complete email security solution can provide what they lack.
- **Consider deploying a VPN** for a more secure connection. This may be particularly helpful with the increase in remote work.
- **Keep backups of your website and database** that you know haven't been corrupted. If your website is hacked, you can restore the website by re-uploading it to your hosting account.

- **Organize your active directory**. Organize Active Directory into a meaningful structure based on the customers' business operating needs. An Organizational Unit structure that provides flexibility to manage computers, users, and former assets or resources allows for quick deployment of network security enforcement changes. Group Policy is a powerful tool for security and incident response alike.



Restrict access to critical data to trusted admins. Giving customers access for the sake of convenience can cause big security problems.

- **Keep administrative access under control**. Remove or minimize use of admin accounts, especially local admin accounts on individual computers. Users with admin privileges are often the entry point of breaches because they have the credentials needed to "unlock the doors." Customers rarely need admin rights. They often just want them for convenience.

- **Identify, isolate, and log access** to critical data. Implement increased logging and network monitoring on the most critical systems. Identity and access management (IAM) systems are becoming easier to deploy and integral to enforcement of security protocols for distributed workforces. Microsoft, Google, and many other IAM vendors exist to help manage access well.

- **Centralize as much logging as is practical**. DNS, DHCP, Active Directory changes, server event logs, firewall and UTM logs, IDS, syslog capture, etc. generate a lot of information. Many RMM and SEIM tools can consolidate the logs and assist with evaluating activity of interest before a risk turns into a breach.

Section 3

COMPLETE YOUR EMAIL SECURITY WITH A SECURE EMAIL GATEWAY

Above all, make sure your email security solution is complete. **Email is often one of the first ways in for cyber attackers**. It can also be vulnerable because you're at the mercy of your users and their ability to discern.

In addition to creating an incident response plan, you need to **make sure your email security solution is complete**. Far too many MSPs and IT security consultants are operating with a partial email security solution. We have seen so many startups create niche solutions and bill themselves as "email security."

Don't allow yourself to be misled by marketing hype and flawed industry trends. **Secure email gateways (SEGs) allow you to control the total flow of email.** If you're using an email security API, it cannot do that without a gateway.

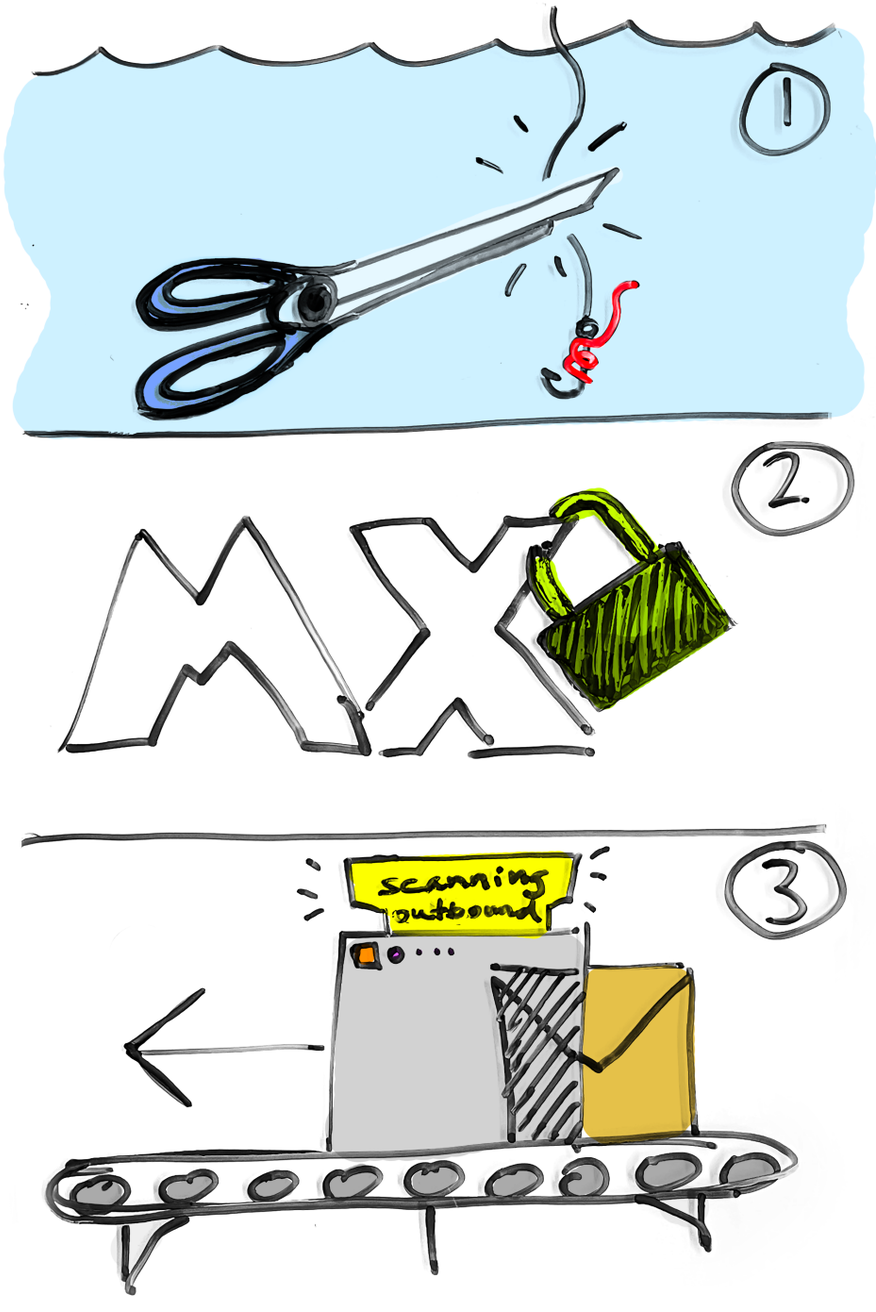
A COMPLETE SOLUTION

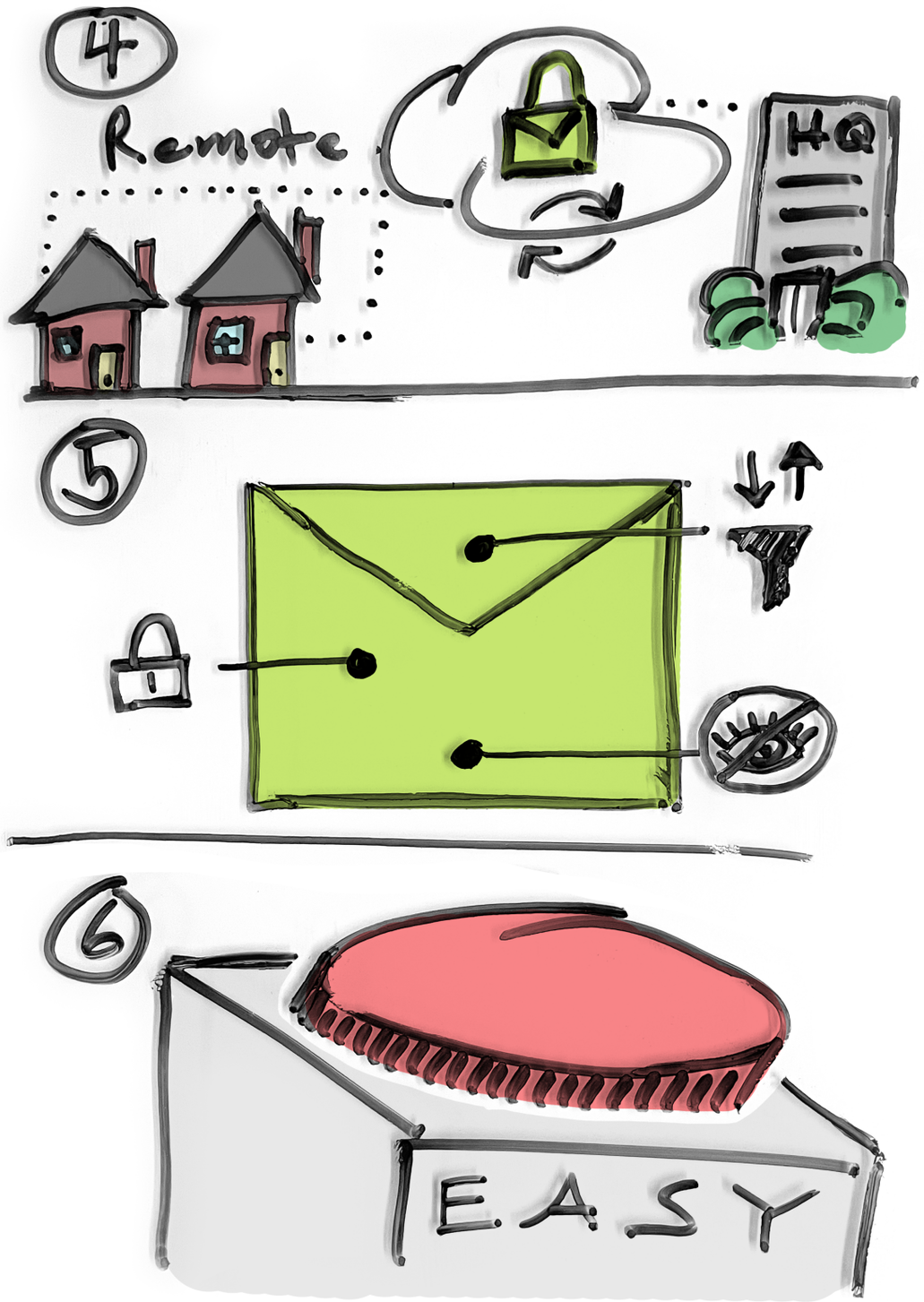
Simply put, email security can't be done halfway. When it comes to email security, you need something more complete than what MS, Google, or an email security API can provide.

1. **Protects from common phishing and malware threats**
   Threat protection is now table stakes, so if your email security solution doesn't protect from phishing and other attacks, you should be looking elsewhere.

2. **Never leaves your MX records exposed**
   This creates unnecessary vulnerability. If the location of your email hosting is exposed by your MX records, it is going to be prone to attacks.

3. **Includes robust outbound email protection**
   Total email security requires the protection of both inbound and outbound email – rather than partial solutions that only protect on the inbound side. For example, what if just one of your users accidentally forwards a malicious or virus-laced email?





4. **Users can safely send encrypted messages and files**
   With the amount of sensitive information being passed amid the bourgeoning hybrid work model, where employees are regularly going inside and outside of your perimeter, it's up to you to keep your customers' sensitive data from being exposed.

5. **No security gaps**
   When it comes to email security, you need something more complete than what Microsoft, Google, or an email security API can provide. **The boxes you need to check are inbound and outbound filtering, email encryption, and email privacy.**

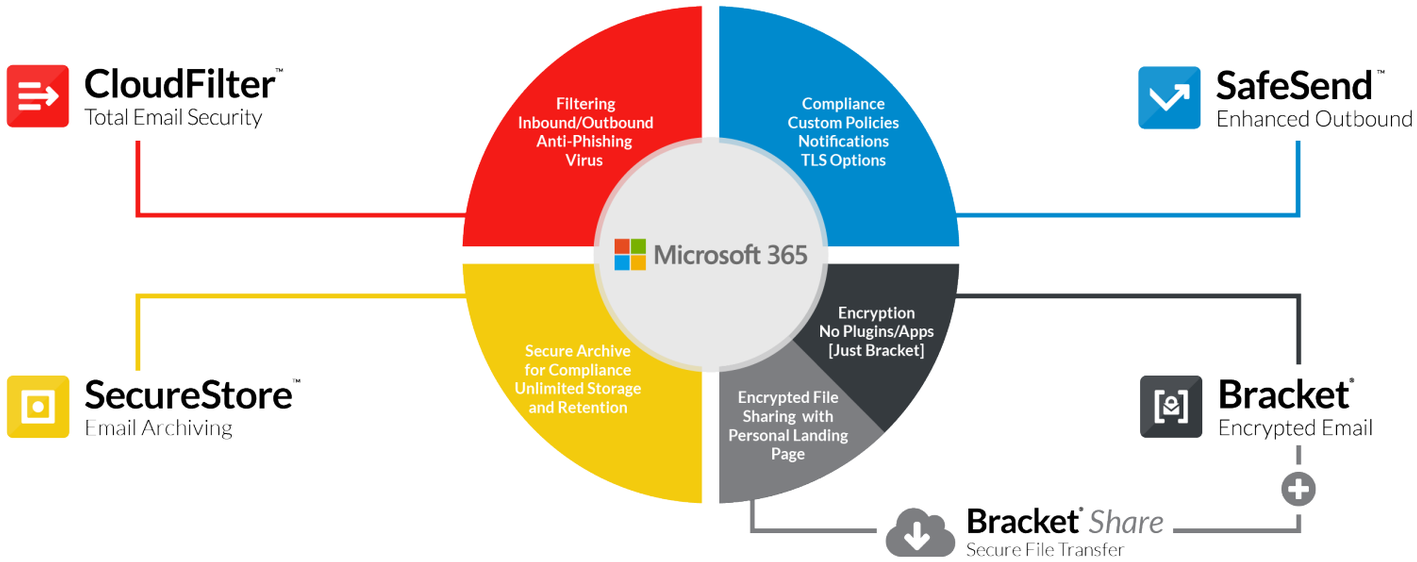
6. **Users find it easy to use**
   That may seem silly but think about anything that makes your job more difficult. The tendency is to find ways around it or stop using it altogether. Security has a reputation of being difficult. So, make it easy, and users will follow the best practices without much consternation.

mailprotector®

Where to start?

SECURE EMAIL USERS WITH MAILPROTECTOR

→ Visit mailprotector.com to schedule a demo today.



During a crisis, **you can only rely on the systems and processes in place prior to the incident**. Your future self will thank your past self for giving this the time and effort it deserves.

We ask that as you're building your plan, you consider email security. Are you using more than the standardized Microsoft- or Google- provided tools? Does your vendor's support department expect to be speaking with an MSP when they answer the phone?

Ours does. Since 2000, Mailprotector has poured itself into perfecting a **secure, intuitive, and easily-administered** set of email security, compliance, and encryption solutions. These were developed in tandem with our global IT security partners and their base of users. Mailprotector customers have peace of mind knowing their end users are secure and happy.