7 ways to keep hackers from destroying your startup

Business

In all fairness, startups have a lot on its plates.

From raising capital to product development to marketing and public relations to just plain keeping sane, startups are typically very busy places. So while your startup may be struggling to balance key elements, likeleadership, staffing, product development, market differentiation and customer acquisition, please understand that its only with the best intentions that we add one more item to your lengthy to-do list - security.

Related:

While many factors, including cost, technical awareness and first-to-market races may make security look like an impediment to growth, it is most assuredly anything but. Some may even argue that by virtue of even claiming an InfoSec department or employee, your company is no longer a startup.

From the earliest stages, firms need to prioritize cybersecurity to ensure it organically evolves in tandem with business, splicing it into the cultural DNA, if you will. In order to develop and promote an organizationally comprehensive understanding of risk as well as policies that will grow with your business, here is a list of seven key security elements that any developing company and its leadership team should adopt.

1. Insist on access management from the start.

No matter how horizontal or egalitarian anenvironmentyou strive to create, not everyone needs to be an admin for everything. The security rule most-oft recommended to startups is to thoughtfully assign services, and then individual logins, instead of sharing the same username and password across an entire company.

Why? Because all companies - no matter how generous your flex-time policy or innovative yourtechnology-- experience turnover. Founders should never be forced to scramble to change access for all personnel each time an individual departs, particularly in the case of a disgruntled employee - or soon to be ex-employee -- who has access to your proprietary and critical IT, IP and other key data. When properly applied, access management allows startups to tailor permission levels, and our recommendation is to dole them out sparingly.

2. Enforce two-factor authentication (2FA).

Two-factor authentication is exactly what it sounds like - the requirement of a second level of authentication in addition to a username and password -- usually in the form of a token with a numerical code, a smart card, a text message to a phone or even a biometric (think thumbprint) scan.

2FA is especially for critical systems like email, Git repos, databases and cloud providers. Requiring a password and a device - what you know and what you have -- can halt a bad actor before they can break in, and let you know something is wrong early on. Imagine being able to thwart the damage caused by credential theft from a spear-phishing attack or malware -- that’s the beauty of 2FA.

3. Use a password manager like 1Password.

It’s 2016. No two passwords should be the same, and there’s no reason to have a password with fewer than 25 characters - letters, numbers and characters. So in addition to 2FA, insert a into your company’s security policy. Password managers are software services that generate and securely store long, complex passwords in an encrypted virtual container. Its beauty is that employees need to remember only one - hopefully robust -- password to unlock the manager, from which they can then cut-and-paste or auto-fill into individual sites and services. Password managers solve the problem of complex passwords for all the sites you use on a daily basis. Make sure everyone in the company uses one.

Related:

4. Use your phone.

Train employees to call whenever a request for sensitive data or materials, like wire transfers, passwords or personnel data, are requested from another party. It doesn’t matter if the request is coming from the email address of someone you share a cubicle wall with. When someone actually does need access to a service - say, they need your 2FA code to get into Twitter -- and they send a note to you asking for those credentials, call and speak to them. Especially at a small startup, where you know everyone’s voice, verbal confirmation is the most effective way to avoid getting phished.

5. Use GPG encryption for sharing sensitive information.

works great for Mac, and you should be using encryption for more than just your emails. Even if your company communications are happening behind

2FA, and logins with complex unique passwords, bad things can still happen. If you’re sharing any sensitive information, encrypt it because if another party is phishing you, they get nothing without the intended recipient’s private key. And if the communications service provider - email, Slack, etc. -- gets hacked, you don’t have to worry about your critical keys being stolen.

6. Use full-disk encryption.

Modern operating systems, such as macOS, Windows 10, iOS and Android, come with . Use it, and make sure everyone else in your company is using it.

iPhones get lost. People leave laptops alone oncoffee shoptables. Tablets are stuffed into airplane seat pockets and forgotten. Stuff happens.

These machines have your company’s intellectual property, strategic plans and access to email, keys and communications, essentially the lifeblood of a tech company. Likewise, make sure your devices require passwords to turn on and wake from sleep. I’d encourage you to encrypt backups too. This comes as a feature on modern operating systems too so someone can’t pick up your external hard drive and wander off, or make a copy while you’re away from your desk.

7. Don’t lose your IP over a latte.

Startups, with their flex-time and work-from-wherever attitudes are awesome at giving employees the freedom to do their jobs from wherever they want. And hey, why not, since there’s free wi-fi practically on every corner - for a price.

Ever hear of ? It’s a free program that lets hackers grab cookies from non-encrypted code, and gain access to your private information. That means can potentially access that individual’s - or even their company’s -- Facebook, Twitter and LinkedIn accounts.

Worse, hackers will set up rogue-yet-legit-looking wi-fi hotspots - i. e. beware anything called “ Free Public Wi-Fi” -- so when you connect to the company VPN over a skim double-macchiato, they can see any data you share and receive over this connection. The solution - read the list above, paying close attention to 2FA, encryption and even tethering to your phone as a hotspot, if your data plan and battery can support it.

Better yet, subscribe to a Privacy-as-a-Service platform, like , which encrypts both data and connections for all employee daily browsing, email, file transfers, messaging andsocial media, segmenting and isolating each device from neighboring users.

And here's a bonus tip. Not to be Captain Obvious, but please: Don’t click sketchy links or download weird things from the Internet, and do study up on your .

Related:

This one should almost go without saying, but it’s really important so I’ll put it here anyway. The Internet is full of nasty stuff, and people with bad intentions. is essential for keeping your data safe. Train all employees to cultivate a healthy amount of skepticism when downloading software. Keep an eye out to make sure website SSL certificates are valid. And install a high quality anti-virus scanner, even Mac users. You never know.