

667 views | Oct 9, 2020, 08:00am EDT

Five Ways To Secure A Work-From-Anywhere Environment



Jim Alkove Forbes Councils Member

Forbes Technology Council COUNCIL POST | Paid Program
Innovation

f *Jim Alkove is the Chief Trust Officer at Salesforce, where he's responsible for enterprise-wide information security and compliance.*

in



GETTY

Five Ways to Secure a Work-From-Anywhere Environment

Jim Alkove is the Chief Trust Officer at Salesforce, where he leads information security, compliance, management and strategy to deliver the world's most secure and trusted enterprise cloud. He serves as an Advisory Board member of the World Economic Forum Centre for Cybersecurity.

When COVID-19 closed offices worldwide, it created a new urgency for organizations of all kinds and sizes — and particularly the CIOs, CISOs and IT leaders within them — to secure their remote work environments.

And as the need for remote work grew, so too did [the threat landscape](#). For companies not born in the digital age, it was overwhelming to juggle their first cloud migration while conjuring overnight a new kind of security posture that met Internet scale-levels of trust and performance. Where those businesses left gaps, often as a result of human error, cybercriminals were happy to [exploit them](#).

As we enter the next phase of our new normal, one where “work-from-anywhere” environments are here to stay, let’s rewind, pause and remember: the [secret](#) to [success](#) is to do common things uncommonly well. Like washing your hands or wearing a mask during a pandemic, nailing the basics to promote [cybersecurity hygiene](#) can go a long way towards eliminating the risk associated with common cybersecurity threats.

So whether you’re a veteran of securing remote work environments or just getting started, here are five important steps you can take to protect employee and customer data:

1. Enable Multi-Factor Authentication (MFA)

Passwords alone aren’t enough to protect against common security attacks. Often, weak or reused passwords are [the weakest link](#) that attackers love to exploit.

As the security landscape evolves, [multi-factor authentication \(MFA\)](#) has emerged as one of the best ways to protect business and customer data. By requiring users to enter two or more “factors” to prove their identity during the login process, MFA [drastically reduces](#) the odds of unauthorized access even if a user’s password is stolen.

For example, accessing to Salesforce products with MFA enabled requires at least two types of factors — a username and password combination, and a verification method that a user has in their possession. We support multiple types of verification methods for MFA, ranging from the Salesforce Authenticator mobile app to Yubico’s YubiKey and Google’s Titan Security Key.

As your cloud migration picks up steam, enabling MFA as part of a [defense-in-depth strategy](#) - vs. relying on employees to brainstorm and safeguard unbreakable passwords - will be a key success factor.

2. Patch Your Devices

Patching corporate devices is a simple, effective, and direct way to ensure employees inoculate themselves against known vulnerabilities, resulting in much improved resilience against common attack vectors like ransomware. Through patching, corporate devices also automatically add necessary new features, remove outdated ones, and fix performance issues. Encourage your employees to patch their personal devices too.

3. Beware COVID-19 Phishing Emails

While [phishing](#) (and its cousin, [vishing](#)) scams are nothing new, the COVID-19 crisis has emboldened cyber criminals to steal personal information by taking advantage of confusion surrounding the rollout of financial assistance and other government programs. As everyday citizens continue to fall victim to these scams, the companies they work for are increasingly affected - either through the loss of productivity or, even worse, stolen business data.

Here again is an example of how nailing the basics can go a long way. And it starts at the top. If CISOs and IT leaders simply raise awareness within their companies of these threats and how to spot them, security-aware employees can render phishing emails and vishing calls ineffective by looking for red flags including:

- Is the subject line off?
- Is the email from a known person or organization?
- Is there anything suspicious about the attachment?

- Is there something phishy about the credentials requested?
- Is the email poorly written?
- Is the message requesting immediate, urgent attention or money?
- Is the call from a familiar phone number?

4. Secure Your Connection Through VPN

Laptops, phones, and, yes, even your smartwatch, connect to the internet with varying (and sometimes random) levels of security controls. By requiring remote employees to use [VPN](#) (Virtual Private Network) on devices with access to business data, companies can dictate the terms of engagement when sending or receiving sensitive information through otherwise public connections.

Put another way: if transporting a briefcase full of cash, would you want a courier driving with the top down and hundred-dollar bills flying all over the interstate? Or would you prefer a secret, secure tunnel purpose-built to keep intruders out? A VPN gives you just that.

5. Secure Your Meetings

With video conferencing at an all-time high, it's more important than ever to review the security settings within your web conference platform of choice. For example, using a platform's built-in security features - such as meeting rooms, passwords and screen sharing permissions - can be basic but critical steps to managing activity and preventing unauthorized access to meetings. Where possible, use unique passcodes and access links for meetings, and disable "beta" features you don't need - like file sharing or live streaming to minimize human error.