OUT IN FRONT PLAYBOOK

JUNE 2023

EMBER
EMBERIT.COM

THE FOLLOWING CONTENT MAY BE CONCERNING

THAT'S WHY WE'RE HERE

As cybersecurity professionals, security awareness is not a box we check, it's our occupation.

For us, cyberthreats and security trends are a healthy obsession. For the leaders and organizations we protect, they are somewhere between overwhelming and terrifying. This fear can lead to doing too little – or worse – nothing. If this sentiment feels familiar, you're not alone.

This Cybersecurity Awareness Playbook is an opportunity to reset, re-commit, or *finally* commit. A chance to shift the momentum, take a proactive security stance, and get out in front of fear and threats.

Our *Out in Front Playbook* is a super-sized edition, spotlighting four security topics of concern to organizations of all sizes and industries. Read on to go beyond MFA, prepare for a passwordless future, further your understanding of ransomware prevention, and explore the ins and out of software updates.

Chris DiFonzo
Chief Executive Officer
cdifonzo@emberit.com

IS MFA PASSÉ?

Implementing multi-factor authentication (MFA) has long been considered a best practice for protecting yourself and your organization against cybersecurity threats. In fact, it's become such a universal element in the cybersecurity toolkit that it's begun to lose some of its value when it comes to preventing threats. Cybercriminals are famously resourceful, so it should come as no surprise that they'd focus their efforts on neutralizing one of our most common and trusted tools. So, does that mean MFA is dead? Far from it. After all, you wouldn't leave your front door unlocked just because someone might be able to pick the lock. It's just not the end-all-and-be-all it once was.

For many individuals and small businesses, MFA is still a foundational step. It is the minimum that should be done to be proactive in your security. Organizations protected by MFA are exponentially more protected than those that aren't, so if your organization hasn't adopted MFA practices, that should be the first step you take – and soon.

For the rest of us, it's time to think beyond traditional multi-factor authentication to what's next. Specifically, to stronger forms of verification like USB security keys or authenticators and certificate based authentication. In both cases, the risk of authentication being compromised is lowered by limiting the involvement of the user in the process. (As we know and have often covered, most security breaches can be traced back to a human factor!). Traditional credential-based networks put the responsibility of security largely on the individual user while USB security keys and certificates help to streamline the process and protect both the user and the organization.

Security Certificate Authentication

By implementing security certificates, your team will remove the need for a password change policy (which comes with the bonus of limiting the onus of internal support tickets) while also adding an additional security layer through public-private key encryption. Security certificates enable your team to identify every connection made within your network, which is a powerful defense against the increasingly popular man-in-the-middle (MITM) attacks that have been popping up to bypass traditional credential-based networks. Where passwords and credentials can be shared – and are thus able to evade being pinned on an individual – certificates put a name to every network connection.

USB Security Key Authentication

At first glance, a physical security key may seem redundant or dated but they possess a number of advantages over traditional (digital) credentials. As we know, even strong passwords are crackable in today's security environment and while code-based MFA is helpful, it is by no means foolproof. Hackers have found ways to bypass these steps as well as intercept them.

Using a USB security key or pairing your password with a USB security key offers an ironclad form of MFA by avoiding reliance on devices in the first place. They provide exclusive and protected access.

Incorporating security certificates, USB security keys, or both, enhances the security practices of your team and provides further safety around access, data, and activity. While traditional MFA is a good start, the advancement of threats means we need to continuously move our own practices forward.

5 WAYS AUTHENTICATION KEEPS *YOU* OUT IN FRONT

No Shared Credentials

Authentication tools like MFA and beyond make it significantly more difficult to share credentials with another team member.

Threat Alerts

Receiving an authentication code that you haven't requested is a clear indication that bad actors are probing your accounts and networks – and a trigger to take proactive action.

More Detailed Access Data

Security keys and certificates allow you to track access back to specific individuals, identifying exactly where threats occur.

Fewer Internal Tickets

Newer systems of authentication don't rely on human intervention to perform password resets and access changes that can deluge an internal support team.

Security on the Go

Authentication helps your team to stay secure even when they're out in the field, which continues to be an issue as both business travel and remote work increase.

IN REAL LIFE

A fabricated-but-plausible cautionary tale

This scenario is a work of fiction. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

Will and Grace are colleagues at a national loan processing center. They've both worked in loan processing for years and have sat in adjoining cubicles for the last decade. Will is a security fanatic, regularly changing his passwords, employing the highest authentication protocols he can, and never sharing credentials. Grace, on the other hand, knows that cybersecurity is a priority but keeps pushing off improvements to her own process and still uses the same password to access loan information that she did on her first day.

One day Will and Grace come into work after a long weekend only to find that all of the private information of their loans has been captured by bad actors. It turns out that not only does Grace use the same password she did on day one — she also happens to use that password across all of her personal accounts (which she logs in to frequently from her work computer). By getting access to her personal email, one dangerous hacker was able to infiltrate all of her personal accounts as well as her employer's sensitive information.

The data breach nearly bankrupts the national loan processing center, but they're able to remedy their security issues by putting in place long overdue processes and training sessions to help their employees practice good cybersecurity hygiene.

Unfortunately, Grace is let go and has to find new work — and new passwords — at a different organization.

EXTRACURRICULAR READING

Click the titles below for further information from resources we trust.

What Is Strong Authentication? (With Examples & Methods)
1kosmos.com // 05.04.22

6 Authentication Best Practices
goteleport.com // 02.25.22

YOU'RE GOING TO WANT TO KEEP THIS PAGE

MOVING BEYOND MFA

Choosing the method of authentication that will be most effective for your can be daunting. That's why we're here. Use this cheat sheet outline some basic parameters and familiarize yourself with the options.

☐ **Step 1: Assess Your Status**

Each organization brings its own unique challenges and strengths when it comes to cybersecurity. It's important to be up-front about where you stand. Ask yourself:

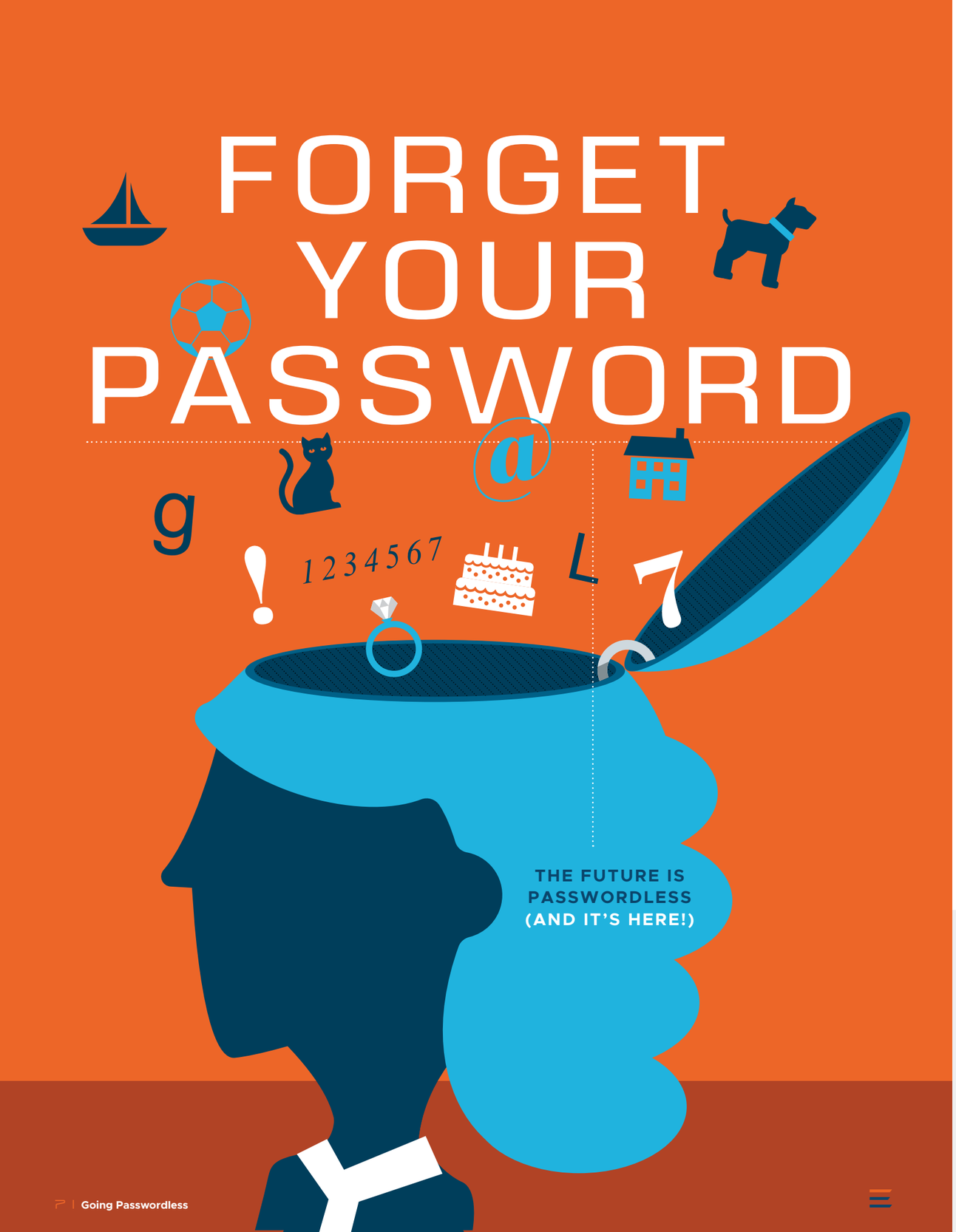
- How tech-savvy is your team? And how open to changes?
- Does your business need to adhere to any Data Compliance Standards, such as HIPAA, or PCI DSS?
- Does your team handle extra-sensitive information, such as medical or financial records?
- Do you have team members that travel or work remotely? What about consultants or freelancers?
- Does your team connect to company resources via a VPN connection?

☐ **Step 2: Meet The Contenders**

Type of Authentication	How it Works	Strengths	Weaknesses
One-Time Passcodes via SMS (OTP)	A user must enter their password and a unique string of characters (usually numbers) sent via SMS as a second form of authentication.	Easy to use Doesn't require additional applications	Isn't the gold standard of security Phones and phone numbers can be stolen or intercepted
Application based authenticators such as Time-Based One-Time Passcodes (TOTP)	Users must enter their password and a time-based, one-time passcode (TOTP) generated by a smartphone application such as Google Authenticator. TOTPs have an expiration window and generally refresh every 30 seconds.	Easy to use More secure than SMS because they use an application rather than a phone number Less expensive than a physical token	Requires users to download and configure a new app on their smartphone May be difficult for less tech-savvy users
Built-in Device Biometrics	Users can verify their identity via the same built-in biometric mechanisms they use to access their device, such as fingerprint scanner or facial recognition. This confirms possession of the device, as well as a biometric marker.	Adds two distinct factors of authentication (possession and biometrics) Resistant to phishing	Account recovery issues can arise if a user loses their device.
Hardware authenticators	Users utilizes a physical piece of hardware, separate from their phone or laptop, to verify possession.	Resistant to phishing	Can be difficult to use for the less tech-savvy Involves purchase of actual hardware devices Can cause delays in account recovery
Client Certificate Authentication	Users authenticate with their password and a digital certificate installed on their device that can be verified by the server or logon service.	Resistant to phishing	Adds management and maintenance time for administrators

☐ **Step 3: Take Action.**

Now that you're ready to make an informed decision to protect ***your*** team, it's time to call ***our*** team.



While we know that strong passwords and multi-factor authentication are necessary when it comes to proactive cyber protection - we also know that – no matter how strong they are – passwords are inherently unsafe when it comes to risk management.

Passwords always offer a way in for bad actors, even with authentication efforts and auto generated keys,

Moving beyond passwords — or going passwordless — is becoming more and more common as individuals and organizations look for ways to enhance and tighten their security protocols.

Passwordless authentication essentially works by replacing passwords with stronger authentication methods. How does it work? In a traditional password-based interaction, your individual password is matched against a stored selection in a database to confirm your access. The storing of said passwords is inherently risky. With passwordless authentication, there is a similar matching method but instead of passwords or strings of letters and numbers, other characteristics or information is matched to authenticate your identity — and your access.

With many large and influential companies moving towards passwordless access, the trend will be towards fewer strings of numbers and letters and more emphasis on truly individualized characteristics.

While passwordless authentication isn't 100% foolproof (because nothing is!), it's much more secure than traditional username-password combinations and offers a path forward for securing accounts and information. Passwordless entry also helps to limit credential sharing, supports remote or distributed teams, and puts less of an onus on your internal IT resources.

FORMS OF PASSWORDLESS AUTHENTICATION INCLUDE:

Biometrics:
Using a user's physical traits (like fingerprints or facial recognition) to uniquely identify an individual. Biometrics can also be used in combination to further strengthen authentication.

Magic links:
Sending a one-time, expiry based URL to the user using a verified email address.

Possession factors:
Using short-term codes generated by a third party system (like SMS or authenticator apps) to grant access.

IN REAL LIFE

A fabricated-but-plausible cautionary tale

This scenario is a work of fiction. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

Angela Bennett, a remote QA engineer for an established video game company, is in the market for a new smartphone. She selects the latest iPhone because it offers unique security protection through its built-in facial recognition login and verification. Angela is excited to try out a passwordless existence and make a purchase that will enhance her already strong security practices.

Fast forward two months and Angela is a regular user of her facial recognition authentication system. She also happens to have been given access to an exciting new video game that is the talk of the industry. Scammers hired by the competition are eager to get a look at the new game and have been working to infiltrate Ms. Bennett's systems — with no luck. These bad actors are so intent on getting access to the video game code that they steal Angela's phone, assuming they can break into the system and get access to her credentials. One after the other, the crooks are denied access due to incompatibility with Angela's facial recognition setup. Angela does have to buy a new smartphone but the game remains secure.

EXTRACURRICULAR READING

Click the titles below for further information from resources we trust.

The Importance of Phone Software Updates and Tips to Keep you Safe
quokka.io // 08.04.22

Want to avoid a cyberattack? Stop ignoring those pesky software updates.
washingtonpost.com // 03.01.22

Understanding Patches and Software Updates
cisa.gov // 02.23.23

YOU'RE GOING TO WANT TO KEEP THIS PAGE

THE HUMAN FACTOR: GOING PASSWORDLESS

PLAYBOOK

5 TIPS TO KEEP YOU OUT IN FRONT

It may seem daunting to go passwordless — especially for a larger or distributed team — but moving beyond traditional authentication is the way of the future. Here are five key steps to moving your organization and yourself past the password.

PICK A METHOD

There are a number of ways to go passwordless. The first step is choosing your preferred authentication factor. Consider the overall security of each method as well as the barriers to adoption for your team. While you want to implement these authentication methods, they won't be useful if no one complies.

OUTLINE YOUR TIMEFRAME

With many cybersecurity updates, it's easy to lose track of the time you're putting into implementing them. Outline a timeline that is firm and works for your team and identify action owners to help you accomplish the task.

PROVIDE NECESSARY TOOLS

You may need to add additional equipment or resources to support your team in going passwordless. Outline what's needed and how you'll go about implementing these resources. (And make sure you're notified of any need to update!).

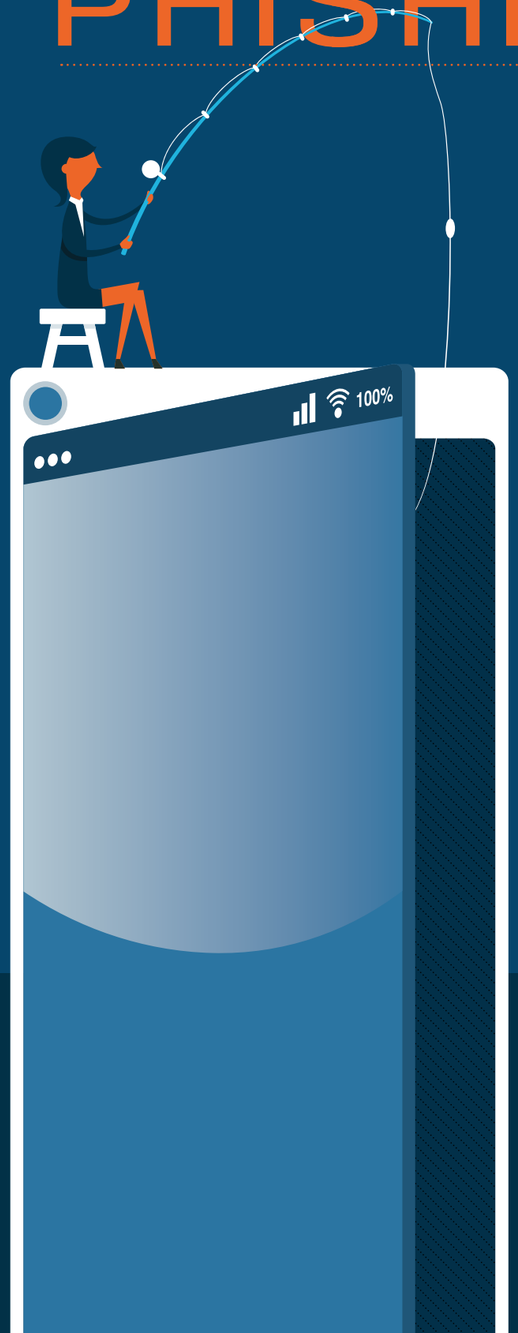
TRAIN USERS

Going passwordless may feel strange for some individuals. Help them by outlining the whys and whats behind this change and clearly identifying key training opportunities. Identify an internal resource to assist with implementation and to answer any lingering questions.

CREATE A PLAN FOR FUTURE UPDATES

It may not be possible to go 100% passwordless right away. Be sure to identify any lingering tools or systems that don't comply and work on a plan of attack to bring every user and every system into the fold.

THE PHUTURE OF PHISHING



IT'S NOT JUST FOR EMAIL ANYMORE

Though cybersecurity threats are ever-evolving, phishing remains the most popular attack method used by hackers to deliver ransomware to individuals and organizations. It is the 4th most common and 2nd most expensive cause of data breaches. Like other cyber threats, phishing attacks are ever-evolving to stay ahead of protections, even going so far as to implement attacks outside of email. Staying current on phishing trends — and what to do about them — is an important step for teams of all sizes.

Here's what to look out for:

INBOX

Bulk phishing — Bulk email phishing is the most common type of phishing attack wherein an attacker creates a message that appears to be reputable and sends the messages to as many people as possible.

Spear phishing — Spear phishing is a phishing attack that targets a specific individual, typically someone with privileged access.

Business email compromise (BEC) — A phishing attack focused on tricking employees or teams into sending valuable assets or information. **In 2022, the FBI received 21,832 BEC complaints, with estimated losses totaling more than $2.7 billion.**

MAJOR THREAT ALERT

[Source: Page 11 of the FBI report: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf]

OUT OF THE BOX

SMS phishing (a.k.a. smishing) — An attack that utilizes text messaging to target recipients.

Voice phishing — Voice phishing are attacks that take place over phone calls, often utilizing voice over IP (VoIP). These calls often mimic calls from credit card companies or the IRS.

Social media phishing — Social media phishing uses various aspects of social media platforms to push for sensitive information. Scammers use in-platform messaging, posts, or emails to target users.

In-app phishing — In-app phishing is a specific type of email phishing where attackers mimic notifications from popular apps and web applications to target users.

It can be tempting to think of phishing as only a big company problem — and only a threat in an email environment — but small business and individual phishing are on the rise, as are attacks outside your inbox.

Read on for key strategies to protect yourself across platforms. ➤

IN REAL LIFE

A fabricated-but-plausible cautionary tale

This scenario is a work of fiction. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

Tony and Carmela are independent consultants who each work with a number of individual clients as well as share a few projects between them. As consultants, they have access to a large number of email addresses, proprietary software, and client-specific accounts. They spend their days bouncing between projects and have set up MFA where possible to keep themselves and their clients safe.

Unfortunately, they sometimes move too quickly for their own good. Tony is in the middle of a large, demanding project and doesn't happen to notice that an email from his client seems uncharacteristically urgent. He clicks on the link his client has sent and finds his entire computer overrun with malware.

The bad actors use this opportunity to send out phishing emails from Tony to his entire email (and client list) while he's recovering from his own phishing mistake.

Carmela receives one of these emails and quickly identifies it as a phishing attack. She marks it as such, lets Tony know that he too has been compromised, and does a quick check of her own data to make sure everything is still secure. Because they have always been security minded, Tony is able to protect his clients from the malware he has downloaded — but he does miss a deadline, spending an entire two day period recovering from the attack.

EXTRACURRICULAR READING

Click the titles below for further information from resources we trust.

The Future of Phishing: Deep Fakes, Coronavirus, US Elections & More
VPNRanks.com // 03.04.22

Five Cybersecurity Predictions for 2023 by Forbes
forbes.com // 01.24.23

The hybrid state and future of phishing explained
i-scoop.eu

YOU'RE GOING TO WANT TO KEEP THIS PAGE

THREAT SPOTLIGHT: PHISHING

PLAYBOOK

5 TIPS TO KEEP YOU OUT IN FRONT

Phishing is a lucrative business for scammers — and with phishing attempts on the rise, it's getting more and more lucrative every year. With phishing extended beyond email, it's important to stay on top of common trends and behaviors across channels to help you identify and address suspicious messages. Here are some key ways to identify a phishing attempt regardless of the platform.

BEWARE AN UNKNOWN SENDER

While phishing attempts are unlikely to come from your partner or colleague, they are likely to come from someone *pretending* to be those close to you. Make sure to pay close attention to names, email addresses, phone numbers, and handles to weed out copycats.

CHECK FOR MISSPELLINGS AND GRAMMAR ERRORS

Similarly, most phishing attempts will feel close to normal, with some obvious errors. Keep an eye out for misspelled names (including your own), grammar errors, or unusual sentence structure.

WATCH FOR SUSPICIOUS LINKS OR ATTACHMENTS

Phishing attempts are built around the goal of getting you to click on a nefarious link and/or offer up confidential information. Keep your eyes peeled for suspicious attachments or unusual links that may contain a virus or malware.

TAKE YOUR TIME

Bad actors are looking for you to take action — and quickly. Most phishing attempts rely on a created deadline or sense of urgency to make recipients act. If a communication feels unnecessarily timely, take a moment to step back and review. Similarly, if a communication is requesting sensitive or personal information, consider that a red flag.

BRING IN SOME BACKUP

Even the best training isn't foolproof. Make sure to implement spam filters on your inbox, manage permissions on social media, and install software where possible to help weed out any phishing attempts that sneak through your defenses.

In the world of cybersecurity, it's a constant battle to keep up defenses and stay ahead of evolving threats.

We see software updates as truly the bare minimum when it comes to protecting yourself — but we also know it's easy for things like software updates to slip amidst all of our other tasks. The problem with letting things like software updates fall to the side is that it leaves you and your organization open to many cybersecurity threats.

Software updates may be triggered by new features or product updates, but they also include new cybersecurity patches made to proactively protect the user. Without enacting these updates, you're actively putting yourself at risk. Ensuring that your software updates are current helps give you the best version of each tool in your arsenal — and strengthens your security. Pro Tip: Limit your tools to only the software you truly need. This instantly reduces the attack surface of your organization.

We now know that hackers actively look for software vulnerabilities and security flaws and that many of the most impactful breaches in the recent past have been a result of these vulnerabilities. These weaknesses let bad actors sneak in and allow infections to take place without the victim actively doing anything. Malicious code can take over your device, steal your data, etc. On top of your own risk, this puts your team, your family, and your contacts at risk as well.

Software updates can be tricky to manage when each tool has its own schedule and updates happen in a truly ad hoc environment. Persistent vulnerability management is key to staying out in front. **Implementing automatic updates can help to take the onus off of you and keep you ahead of the game without adding a to do item to your list.**

> ***Or not!***
>
> **Automatic updates aren't always the right answer. Strategically skipping or delaying an update might be the right call depending on your job function, industry, or the specific update.**

Activating automatic updates, prioritizing the tools that matter, monitoring these tools for updates, and setting up update notifications can all help to take the strain off of managing software updates and protect yourself from outside threats. It may seem insignificant but updating software is a critical component to remaining secure.

57%

OF ALL OBSERVED VULNERABILITIES ARE MORE THAN 2 YEARS OLD

17%

OF ALL OBSERVED VULNERABILITIES ARE MORE THAN 5 YEARS OLD

Source: PRNewswire

IN REAL LIFE

A fabricated-but-plausible cautionary tale

This scenario is a work of fiction. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

Michael Cutter is a CTO at a growing startup focused on building mobile applications for healthcare. While he is a highly skilled and dedicated technical professional, he's also a consummate early adopter, constantly downloading and testing out new tools, code, and gadgets (and not always from the safest sources). He is a religious updater of passwords and keeps an eye on security trends — especially because his startup is too small for a dedicated security leader — but his early adoption of new technologies creates a security risk that he has yet to notice.

In fact, Mr. Cutter has accumulated such a backlog of discarded tools — on average, one new download a week for the entirety of his three years at the company — that eventually one of them did cause a breach. Six months after it was downloaded (and forgotten), a project management application that didn't quite work for the team let in a piece of malware that exposed millions of healthcare records and tarnished the reputation of Mr. Cutter's startup. The company ended up losing 20% of their users, shortening their runway because of extra cost that had to be leveled on cybersecurity, and negatively influencing their next funding round. While the company was able to survive the breach, their growth was greatly impacted.

EXTRACURRICULAR READING

Click the titles below for further information from resources we trust.

What is Passwordless Authentication? Benefits and Challenges
lepide.com // 03.01.22

New Survey by HID Reveals Five Pressing Themes Reshaping the Security Industry
securitytoday.com // 03.23.23

Passwordless login with passkeys by Google
developers.google.com // 05.11.23

YOU'RE GOING TO WANT TO KEEP THIS PAGE

THREAT PROFILE: SOFTWARE UPDATES

PLAYBOOK

4 TIPS TO KEEP YOU OUT IN FRONT

In today's constantly changing work environment it can be difficult to make sure your systems and tools stay up to date — but it's also critical to proactive cybersecurity protection. Creating a repeatable process to stay ahead of updates helps make sure your team is out in front of gaps in security.

ALIGN YOUR TEAM

Keeping tools up to date isn't just about your tools — everyone on your team needs to stay up to date to ensure a secure stance. Schedule regular alignment sessions with your team to catalog and document the tools, systems, and software that your organization needs to function.

PRUNE YOUR SOFTWARE

Once your team has aligned, use this as an opportunity to remove inactive tools, prevent duplicative systems, and address any known issues with your software. Keeping your list of active software programs to a minimum means fewer updates and fewer risks.

ENABLE PROACTIVE NOTIFICATIONS

In today's environment, most tools offer settings that can help to proactively notify you when an update is available. Make sure you have these settings turned on to help identify opportunities to update as they arise.

GET ON SCHEDULE

Each system updates on its own schedule so it can feel overwhelming to keep your systems up to date. While proactive notifications will help, it's also crucial to schedule regular update checks and to appoint a team lead who will be responsible for such checks.

FEATURED PARTNER SOLUTION

With new types of connected devices and digital platforms popping up every day and more tools collecting more data, cybersecurity is an existential risk for all businesses. Tenable's mission is to empower all organizations to understand and reduce their cybersecurity risk and to provide actionable insight to today's leaders.

The old way of simply scanning on-premises IT devices for vulnerabilities is no longer enough. It's time for a new approach. Tenable's solutions offer options for every type of security need and help companies see everything, predict what matters, and act to reduce risk. Their platform gives all the insight, research and data you might need to uncover weaknesses across your entire attack surface and provides continuous, always-on discovery and assessment in order to provide the visibility you need. Built-in prioritization, threat intelligence and real-time insight help you understand your exposure and proactively disrupt attack paths.

40,000 organizations around the world rely on Tenable to help them understand and reduce cybersecurity risk.

OUT IN FRONT OF	Vulnerability Management, Attack Surface Reduction, Compliance
WHAT TENABLE DOES	Tenable empowers all organizations to understand and reduce their cybersecurity risk.
INDUSTRIES SERVED	■ Energy ■ Healthcare ■ Retail ■ Water ■ US Federal ■ Medical Manufacturing ■ Automotive Manufacturing ■ Building Management Systems ■ Finance ■ Oil & Gas ■ Transportation ■ State/Local/Education
KEY FEATURES	DISCOVER: Identify vulnerabilities. ASSES & COMPLY: Understand risk. ANALYZE & REPORT: Secure the modern attack surface.
BEST FOR	Organizations with complex environments and stringent regulatory requirements

EMBER™

Delivering best-in-class cyber security, IT management, and consulting services to small-to-mid-sized businesses

EMBERIT.COM