ACT SMART I.T.
Helping You Benefit From Today's Technologies

February 2023 BUSINESS EDITION

Why You Need A Password Policy

Everyone should have a password policy. Your business' policy should be formal, written and signed by everyone in your company to acknowledge that they know and understand that policy.

An individual or family should have a "policy" as well; guidelines that they follow to help keep their personal information safe.

Passwords are part of every organization's security risk profile that should be taken seriously by everyone. Just one weak password with access to an organization's critical systems can cause a breach, take down a network or worse. Whether we like it or not, passwords are here to stay as a form of authentication for at least another decade or so. There is no time like the present to review your organization's password policy and update it for the betterment of your organization's overall security.

Your personal and enterprise passwords and policies should follow these recommendations. The reasons your passwords and password policies should follow these recommendations are due to the methods attackers commonly use to compromise passwords and the defenses it takes to mitigate those threats.

Passwords and password policy comes down to risk acceptance and individual risk decisions.

But, aren't passwords going away?

The end of passwords is coming soon" prediction is a frequent theme in cybersecurity that never seems to arrive. If you look at the sheer amount of passwords that the average person still uses today, a passwordless world is either never going to happen or at the very least, likely to be a decade or more off. This is despite nearly universal agreement among cybersecurity experts that passwords are too easy to compromise and that something better needs to replace them. Today's conventional wisdom is that multi-factor authentication (MFA) needs to be used wherever possible to better secure logins until something more advanced, like "zero-trust" security architectures, can be implemented at scale to replace passwords forever.

What is Zero Trust? Wikipedia has a pretty understandable definition that is too long to quote here.

Although the number of passwords that the average person has varies by study, most say the average person has between 7 and 191. passwords.

Far from being a passwordless society, today, most of us use a combination of multiple, unrelated MFA solutions and multiple passwords to authenticate to various sites and services. The average user often has one or more MFA solutions (e.g., for work, banking, stocks, social media sites, etc.), plus a whole lot of passwords all to manage at the same time. So, until something changes drastically in the digital world, most of us are going to be stuck with a whole bunch of passwords to create, use and manage.

If users create and use passwords in a way that minimizes hacking attacks and if the systems that store them protect them so they are not accessed or guessed by attackers, they can be a secure way to log in. Passwords are fairly easy to use. Everyone quickly learns how to use them.

But there are reasons why nearly all cybersecurity experts agree that passwords need to be replaced with something better. Passwords are also fairly easy to steal, hack and guess. Why? Here are some of the reasons:

- It is difficult for humans to create strong passwords that withstand common password attacks
- Newly created passwords are easy to forget
- Passwords can easily be reused across multiple, unrelated websites and services
- Passwords are easy to share with other people
- Passwords are difficult to manage when you have many
- Passwords can be easy to guess if not enough complexity is required and/or if
- the login portal does not limit the amount of guesses
- And, of course, the worst problem is that passwords are easy to steal .

There are many ways to compromise passwords. In general, the various password attacks can be summarized as:

- Password theft
- Password guessing
- Password hash theft and cracking
- Unauthorized password reset or bypass

(Continued on page 3)

Welcome February!

This month, we start our video challenge; to create at least one video a month. First, we had to "get over ourselves!" and realize that we will never be perfect, poised and natural while recording. Pam's first video "Phishing 101" of our new, monthly "Coffee Break" series only has her voice and even that was nerve wracking, she said.

She did find a easier way to record, though. Originally, she was doing a recorded Zoom meeting with a shared PowerPoint presentation. Take after take, she said she flubbed something and had to start over.

Then, she realized that she could video the PowerPoint with her voice over! With trial and error, she found that she could go slide by slide so, when she flubbed, she could go back and re-record. She was even able to go back to an individual slide after she finished recording, if she found that something wasn't quite right.

You can choose to be shown in a small box on the screen as you record or not. She chose not to be shown for this one but may get braver and allow it in the future. Take a look and see what you think: **ACTSmartIT.com/coffee .** I think she did a pretty good job.

I'm sharing this info in case you've been considering doing videos for client educational purposes or to introduce new products, procedures or team members.

I have a video that I want to create and her new method might make me a little more comfortable. As they say, I have a face for radio!

After all the breaches recently, I suggest that you change your passwords. I know, a HUGE task! Companies seem to wait weeks or months before they announce the breach and you'll have peace of mind that you have already changed your password.

In you business, and even in your personal life, having a password policy is a smart move. That way, everyone is aware of the most secure and safest way to use passwords. You can find our suggested policy, thanks to KnowBe4.com on our page ACTSmartIT.com/password-policy.

And, to keep all these passwords straight, use a password manager!
Looking forward to SPRING!

Why You Need A Password Policy

(Continued from front page)

These methods are used millions of times a year by various threat actors. The methods can be used by a single threat actor to obtain one or more passwords for their own uses, for reselling, or to populate larger login credential lists that can be used, viewed or sold. Today, there are many existing "password dump" stolen password lists available on the dark web and Internet that contain millions to billions of previously compromised passwords.

With tens of billions of login passwords available for viewing or buying, there is a growing chance that over time, nearly everyone will have a login credential stolen and placed on one of these password dump lists.

All stolen passwords were at some point, uncompromised, and only known by the user and the involved authentication system (and possibly other authorized parties), but somehow subsequently became compromised by unauthorized attackers .

The theft of passwords from victims can occur many ways, including:

- In-person
- Social engineering
- Hackers or malware on the endpoint
- Network eavesdropping
- Stolen credential databases
- Visible in publicly accessible code

Not Easily Guessed

No matter what the other password policies are, passwords should not be easily guessable. This means that they should contain:

- Minimum password length (say eight characters)
- Moderate amount of required complexity
- Not be an old password that the user has previously used
- Not be composed of their name or login name
- Not use any passwords previously identified as "common passwords"

WHAT YOUR PASSWORD POLICY SHOULD BE

With everything discussed, password attacks and defenses against them, this is what your password policy should be.

Use MFA (Multifactor Authentication) wherever you can

Use MFA and/or long passwords / passphrases to logon to your devices and change passwords at least annually

Use a password manager and protect it with MFA and long password/passphrase

If you must create your own passwords, make them long (20+ characters)

Optimally: MFA+ Password Manager + 2 long password/passphrases (1 for each device and password manager)

Passwords are likely to be with us for some time, probably a decade or more. The types of attacks against passwords (e.g., social engineering, theft, guessing, hash cracking, bypassing, etc.) have not changed that much over the last two decades.

However, so many passwords are successfully stolen, guessed, and cracked each year that moving to another, better form of authentication is needed. But until passwords are completely replaced, you need to create and manage your personal and professional passwords to minimize risk of a successful attack.

Don't Overlook The Importance Of

In recent years, the importance of UX design has become increasingly evident. Companies are now investing more in UX designers to create user experiences that are both enjoyable and effective. By understanding the needs of their users, companies can deliver products and services that meet those needs and ensure a positive user experience.

What Is UX In Web Design?

UX design is not just about visually appealing interfaces; it involves evaluating how well they function and meet user needs. UX designers must consider usability, accessibility, performance, and overall user satisfaction to ensure that the product or service meets the expectations of its users.

UX design often comingles with other disciplines, such as graphic design, interaction design, and information architecture. Each of these disciplines is essential in creating a successful user experience. Combining their efforts, UX designers can develop products and services that engage users and meet their needs.

Why Does UX Design Matter?

Good UX design can differentiate between a successful product and one that fails. Companies that invest in UX design can create products and services that users enjoy using, which leads to greater user engagement and higher customer satisfaction. As a result, it can increase companies' sales and profits.

Some examples of successful UX design include Instagram, Netflix, and Amazon. All of these services focus on the user. As a result, the sites and apps are easy to use and understand, contributing to their success.

What Are The Applications For UX Design?

Website owners can apply UX design to increase interaction. UX designers must consider all aspects of the user experience throughout the design process. Components include usability, aesthetics, navigation, responsiveness, and feedback.

Usability - A successful UX design will enable users to interact with the product or service quickly and efficiently. Examples include strong calls to action on websites, intuitive navigation for mobile apps, and quick loading times for games.

Aesthetics - First impressions are essential, and aesthetics play a vital role. From choosing the best color swatches, fonts, images, and icons, UX designers must ensure that everything is visually appealing while meeting users' needs.

Navigation - UX designers focus on streamlining the navigation process for visitors, simplifying the user journey and allowing them to find what they need quickly and easily. By prominently displaying the key actions and features, they can direct users to the right places.

Responsiveness - UX designers must ensure that their designs are responsive to different devices and platforms. Creating fluid experiences across desktops, tablets, mobile phones, and other devices help ensure the broadest appeal.

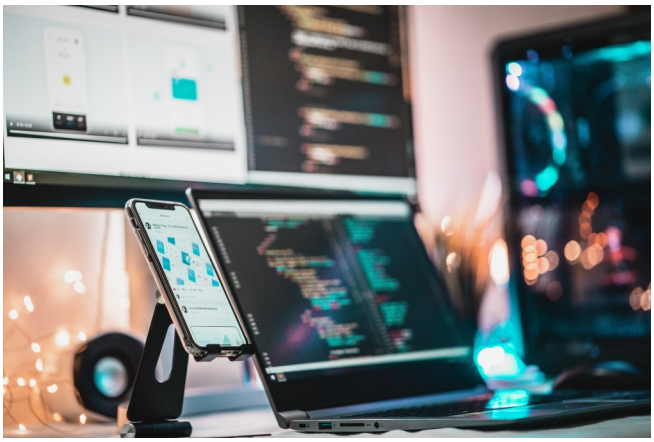
Feedback - Feedback loops are essential for a successful UX design. By understanding how users interact with the product or service, designers can tweak it to meet their needs and ensure a positive user experience.

Why Everyone Should Care About UX Design

UX design is essential for any product or service that requires user interaction. It ensures users can interact with the product enjoyably and effectively, leading to higher engagement and satisfaction. Everyone should care about UX design because it can make a massive difference in the success of a product or service. Even minor tweaks to existing designs can considerably impact user experience. For any company or organization that wishes to succeed, focusing on UX design is essential.

UX (User Experience) In Web Design

Good user experience can significantly increase sales and profits for businesses, making it an essential in-



vestment for any product or service. In addition, investing in UX design helps companies create loyal customers who come back repeatedly, helping to ensure long-term success.

As it applies to UX in web design, the top deliverables UX designers produce are wireframes, user flows, task analysis, and information architecture. These frameworks and outlines help to create a cohesive and consistent user experience by ensuring that all pieces work together to provide the most efficient path to reaching the user's goal.

Wireframes and user flows help designers map out the visual elements of a website, while task analysis and information architecture allow them to understand how navigation fits into this layout. All of these deliverables come together to create an intuitive experience that is easy to use while meeting user needs.

Evaluating Results Of UX Web Design

When launching a new website, evaluating the results is critical to determine whether the UX design was successful. A website's analytics can provide insights into user behaviors and preferences, allowing designers to adapt their designs accordingly. By seeing which parts of the website are getting used, how quickly users navigate, and the conversion destination, UX designers can determine whether they have achieved the desired outcome.

Data collected from website analytics empowers designers to compare designs to see which works best for the user. A/B testing is among the most effective ways to do this, as it allows designers to compare two designs and monitor their performance over time. This valuable data is vital in identifying which design elements work better than others and making modifications accordingly.

Another approach to improving website users' experience is having people test the site and collect feedback. This process provides valuable insights into how people interact with the website, allowing designers to make necessary improvements.

The underlying technology that powers a website may be pretty complex, but the user experience should always be straightforward. Ideally, visitors shouldn't need to spend a lot of extra time or effort to understand how a website functions—the whole point is to get them to their desired goal as quickly and efficiently as possible.

Improving The UX Can Improve Conversions

By continuously evaluating and refining UX designs, designers can ensure that their websites meet user needs and deliver positive experiences. Moreover, doing so will help create loyal customers who keep returning for more.

If your existing website needs to meet essential business objectives or provide the user experience you desire, Interactive Palette can help you. Our team of experienced UX designers can help develop user-friendly websites that drive conversions and improve customer loyalty. Contact us today to start the conversation.

Kevin McNally, www.InteractivePalette.com
Don't hesitate to get in touch with an expert from Interactive Palette today!
(781) 930-3199 sales@interactivepalette.com

Mobile Malware Has Increased 500%

What Should You Do?

Cybersecurity researchers uncovered an alarming mobile statistic. During the first few months of 2022, mobile malware attacks

surged 500%.

For years, mobile phones have become more powerful. They now do many of the same functions as a computer. Yet, people tend to secure their computers better than they do their smartphones.

This is a behavior that needs to change. Over 60% of digital fraud now occurs through mobile devices. That makes them highly risky if proper safeguards aren't followed.

Use Mobile Anti-Malware

Yes, your mobile phone needs anti-virus too! Malware can and does infect smartphones and tablets. Ensure that you have a reliable mobile anti-malware app installed.

Don't Download Apps from Unknown Sources

Only download mobile apps from trusted sources. Do not download outside a main app store. Trusted app stores include places like:

-Apple App Store

-Google Play

-The Microsoft Store

-Amazon Appstore

Do not Assume Email is Safe

Many people prefer checking email on their phone rather than PC because it's so handy. But they have a false sense of security about the safety of emails when viewed on a mobile device.

It's difficult to hover over a link without clicking when on a smartphone. If you see something questionable and want to check the link, open the email on your PC where you can do that.

Beware of SMS Phishing (aka "Smishing")

In March of 2022, text spam outpaced robocalls. Unwanted text messages rose by 30%, ten percent higher than robocalls. Many of those spam texts are smishing.

Be on the lookout for text messages that don't quite make sense.

For example, getting a shipping notification when you haven't ordered anything.

Remove Old Apps You No Longer User

Go through your device and remove old applications that you are no longer using. There is no reason to keep them around, potentially leaving your device at risk.

Keep Your Device Updated

Speaking of updates, you also need to keep your device's operating system updated. Are you using the current version of Android or iOS? Not installing updates can mean your phone has vulnerabilties. These vulnerabilities allow hackers to breach your data.

Use a VPN When on Public Wi-Fi

Public Wi-Fi is dangerous. Most people understand that, but many connect to it out of necessity. Reduce your risk by using a VPN app

Mobile Security Solutions to Prevent a Data Breach

Don't wait until your phone is infected with malware to secure it properly. It's only a matter of time before you are the next victim.

Attention Office 365 Users:

Hackers are using a new trick to deliver phishing attacks

According to an analysis by Proofpoint, there's been a rise in cybercriminals attempting to deliver malware using OneNote documents, the digital notebook with the .one extensions part of the Microsoft 365 office suite.

As more people move to use Office 365, these types of attacks are likely to increase because they can more easily bypass threat detection.

This type of phishing email was first seen in December 2022 and targeted specific industries. A few sectors, manufacturing and industrial, received sophisticated phishing emails with attachment names related to machine parts and specifications, indicating a high level of research was put into crafting the "bait."

In January 2023, the frequency of these emails rose significantly, was more generic, and did not target specific organizations or verticals. The criminals knew they had created something that worked, so now it was time to "mass" deploy and catch as many fish as possible.

The emails attempt to deliver malware designed to steal sensitive information, including usernames and passwords. However, based on current research, forensic engineers believe that a ransomware payload is in the works and will be deployed next.

The current email phishing themes and attachments have been invoices, remittances, shipping, and seasonal themes, such as information on Christmas bonuses and vacation schedules.

One thing to keep in mind with this phishing attack is that it relies on the victim (you/your staff) opening the email, opening the OneNote attachment, and clicking on malicious links. OneNote does offer a warning message about suspicious links. Still, users who've been sent a deceptive and well-crafted email (think vacation schedule or payroll/bonus issue) could attempt to bypass this warning.

Important Note: as of right now, an attack is only successful if you/your staff engages with the attachment, specifically by clicking on the embedded file and ***ignoring*** the warning message displayed by OneNote. Please inform your team about this new email threat and encourage them to report suspicious emails and attachments immediately so no one else falls prey.

ACTSmart IT
332 Main Street
Wareham, MA 02571

In This Issue

Know a business who could use this type of information? Send them to ***ACTSmartIT.com/newsletters***

Is a Hacker Using Your Security Camera to Spy On You?

Those doorbell cameras are all the rage. Gosh, you can even feel FOMO if you don't have one.

Neighbors eagerly post camera images warning others that a salesperson is making their way around the neighborhood.

Prices for home security systems have dropped. It's never been so cheap and easy to see who's knocking at your door.

But did you stop to think who is watching you?
Horror stories abound about these DIY security cams. Stories about creeps talking to children. Smarter creeps spy on you silently and steal data.

The problem is that these systems aren't as DIY as we're led to believe. Most consumers don't know a darn thing about securing them. They leave usernames and passwords at defaults. Or if they do manage to change the password, it's something easy. Easy-to-remember often means easy-to-hack.

Here are some tips to keep the hackers out of your security system:

- Secure Your Router
- Change the Default Username & Password
- Ensure the System Uses SSL/TLS
- Keep the Software Updated
- Consider Access Levels for Multiple Users
- Enable Camera Security Features
- Make Sure Your Mobile Device is Secure