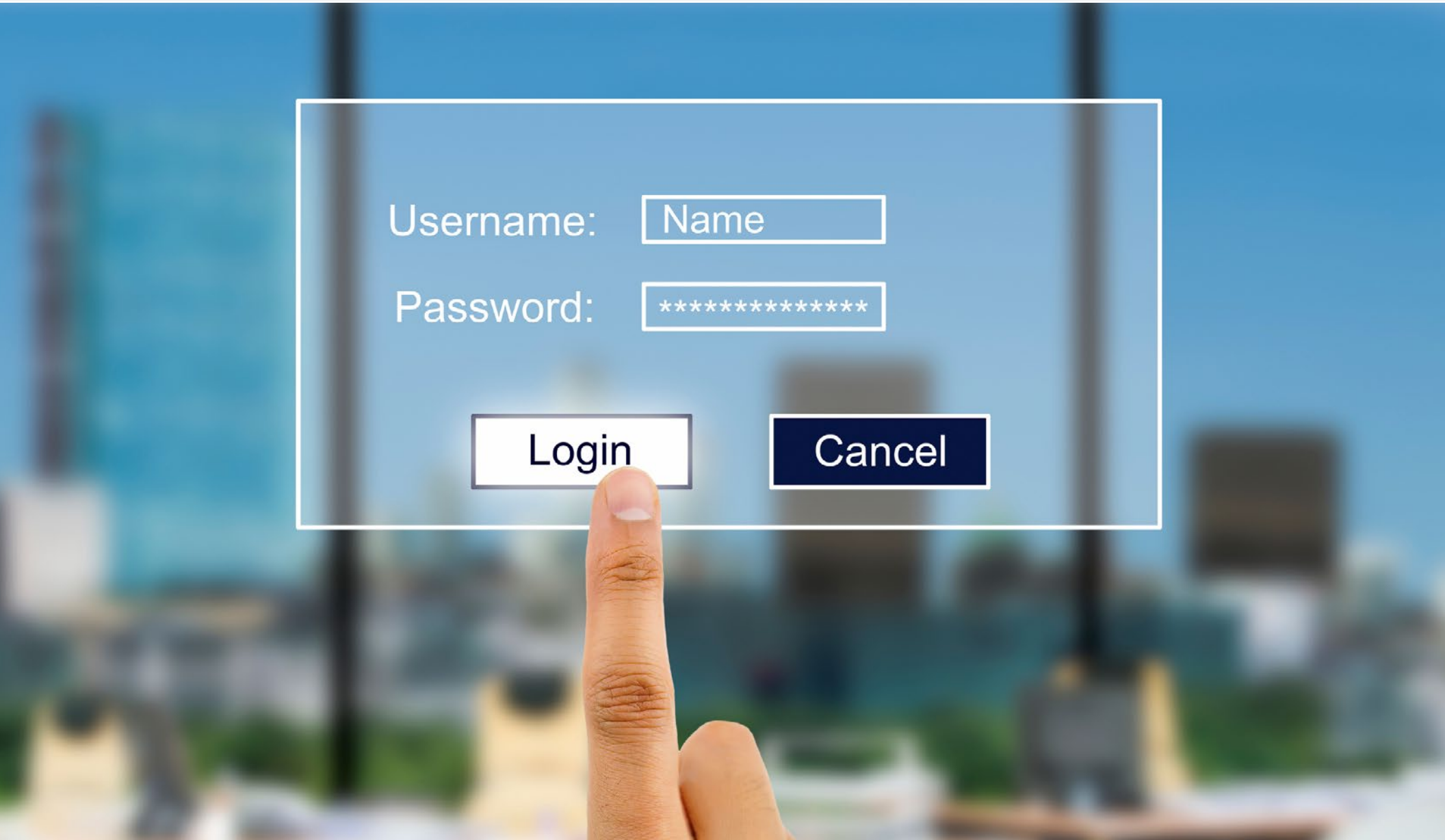
Think HR
Human Powered

CYBERSECURITY
PART 3: AUTHENTICATION



Think HR
Human Powered

CYBERSECURITY
PART 3: AUTHENTICATION

Corporate networks in companies of all sizes are under siege by a growing number of increasingly sophisticated attacks from cyber criminals across the world. These attacks can happen at any time, both to your business or to you personally on your own private networks. There are steps you can take to reduce the risks as the first line of defense against data breaches, malware infiltration and various other security risks.

This is Part 3 in the series of prevention steps you can take to help make your information networks more secure.

Things have changed over the past few years…cyber criminals are now focusing increasingly on you and your fellow users as the weak link in the security chain.

You…

are the primary line of defense in preventing really bad stuff from happening in your company and to yourself.

There is nearly a one in four chance…
that you will mistakenly click on a phishing email.

One click on a phishing email…
could cost your firm $377 per employee.[1]

A single Trojan horse exploit…
caused the State of California to shut down a business a few days after the attack occurred.[1]

One stolen laptop…
from the car of an HR professional who worked for Godiva Chocolatier revealed the names, addresses, Social Security numbers and drivers' license numbers of other employees.[1]

Edition: 4.2116

Poor Authentication Is Risky

What Are We Talking About?

Authentication is simply the process of verifying that you are who you say you are when attempting to access a system. The most common form of authentication is a username and password combination, but there are a number of different authentication methods that can be used:

TWO-FACTOR AUTHENTICATION

This method of authentication requires two different verification modes to gain access to a system. For example, an automated teller machine (ATM) requires you to *have* something (an ATM card) and to *know* something (a Personal Identification Number, or PIN) in order to make a transaction.

OUT-OF-BAND AUTHENTICATION

This access method uses two completely different communication modes to verify you. For example, upon successfully entering a username and password on a desktop computer, a system can then require you to enter a code that it sends to your mobile device.

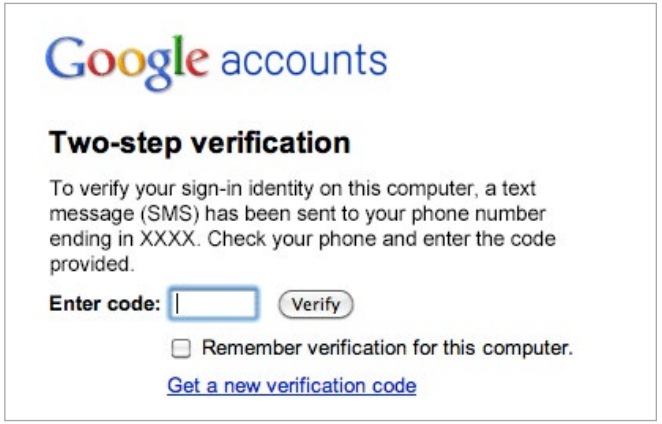


Figure 1: Two-Factor Authentication in Google Apps
Source: Google

CHALLENGE/RESPONSE

This method requires you to answer questions that you previously entered into a system. For example, many banks requires you to a) enter your username, b) answer one of several questions about your personal life, and c) your password. If you cannot answer correctly, you are not given the opportunity to enter your password.

IMAGES OR PATTERNS

Some systems require you to enter letters and/or numbers that are provided in an image after they have entered their username and password. This method of authentication, also known as CAPTCHA[2], can prevent robots or automated dictionary attacks from gaining access to a system because these tools are typically not capable of identifying text in images.

Edition: 4.2116

BIOMETRICS

These methods require you to scan your fingerprint, iris, face, finger length, voice, typing rhythm or some other unique, biological characteristic that is unique to you when attempting to access the system. These systems have the distinct advantage of being difficult to spoof by unauthorized parties, but they can result in false rejections. Some systems are quite sophisticated–for example, the biometric authentication used in Microsoft Windows 10 can detect the blood flow in your face and cannot be fooled even by your identical twin.

Weaknesses in Current Authentication Schemes

While authentication is required in virtually every corporate system, there are a number of weaknesses in some current authentication schemes and/or the way they are implemented by many users and IT departments. Addressing these vulnerabilities is essential for any organization, since 75% of network intrusions are the result of stolen or weak credentials.[3]

You should always use strong passwords when accessing a corporate system.

- Many users employ extremely weak passwords that are easy for cyber criminals to guess. For example, Splash Data found that the five most common passwords employed in 2015 were "123456," "password," "12345678," "qwerty" and "12345."[4]
- Most users do not change their passwords on a regular basis and are not forced to do so by a corporate system. The result is that systems are increasingly vulnerable over time simply because the same password is exposed to cyber criminals for a longer period.
- Most users employ the same password to access multiple systems–a survey of users in the United States and the United Kingdom found that nearly 75% of users do so. While this practice makes it easier for users because they need to remember fewer passwords, it also makes it easier for cyber criminals, since hacking into one system by determining a user's password gives them access to several other systems.
- In some situations, users will share the same login credentials with others, particularly for systems like FTP servers that are not frequently accessed. This makes data breaches easier because multiple people have the same login credentials and because these credentials are often not changed when a user leaves the company.

Edition: 4.2116

How to Defend Yourself

There are a number of best practices that users should employ when accessing corporate systems:

EMPLOY STRONG PASSWORDS

You should always use strong passwords when accessing a corporate system. Typically, the longer the password and the greater the variety of characters it contains (upper case, lower case, numbers, punctuation, etc.), the stronger and more difficult it will be to hack.

To demonstrate the relationship between the strength of a password and the length of time required to crack it, we ran five passwords of various strength through the password checking site howsecureismypassword.net. The amount of time required for a desktop PC (performing four billion calculations per second) to randomly crack each password is shown in *Figure 2*.

Password	Time to Crack	Character Combinations	Possible Combinations
happy	< One second	26	11 million
happy9	0.54 seconds	36	2 billion
happy99	19 seconds	36	78 billion
happy99K	15 hours	62	218 trillion
Happy99K)	275 days	77	95 quadrillion

Figure2: Comparative Strength of Passwords

Source: Small Hadron Collider

Obviously, a hacker could probably make more educated guesses if he or she was attempting to crack your password, but the example above demonstrates that stronger passwords create more of a barrier for cyber criminals.

CHANGE YOUR PASSWORDS FREQUENTLY

While some systems and IT administrators force a change in passwords on a regular schedule, you should routinely change your password without prompting. Setting a calendar reminder, for example, to change passwords every 90 days can help to reduce the likelihood that your passwords will become compromised.

Edition: 4.2116

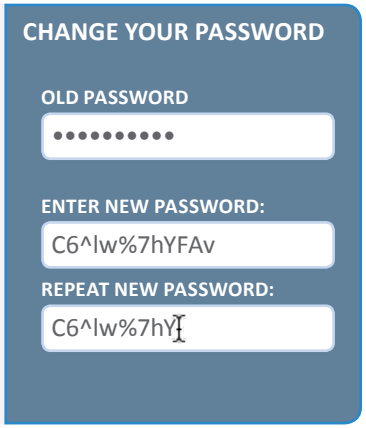
USE A UNIQUE PASSWORD FOR EVERY SYSTEM

The common practice of using the same password across multiple systems increases the opportunity for a cyber criminal to hack one password and thereby gain access to multiple systems. Best practice is to use a unique, strong set of login credentials for every system.

INTENTIONALLY USE WRONG INFORMATION FOR SECURITY QUESTIONS

Some systems, particularly those that ask users to answer a variety of security questions during the initial set-up, will ask for information like your mother's maiden name, the name of your first pet, the city in which your parents were married, etc. Because this information might be requested by a variety of systems, providing the "wrong" answer to these questions, and providing different wrong answers for each system, can reduce the likelihood of a cyber criminal being able to respond to security questions correctly.

While some systems and IT administrators force a change in passwords on a regular schedule, you should do so even without being prompted.



EMPLOY AUTHENTICATION APPROPRIATE TO THE SENSITIVITY OF THE INFORMATION

In most cases, IT will establish the level of authentication required for you to access a system, but you often have some control, particularly for personally-managed cloud applications and the like. For example, Dropbox allows you to set up two-factor authentication that requires not only the input of your username and password, but also a six-digit code that is sent to your mobile device. This extra level of authentication, while not 100% secure, makes it more difficult for cyber criminals to access your Dropbox account because they would need both your username/password combination and your mobile device.

USE A PASSWORD MANAGER

For companies that have not implemented single sign-on capabilities, the use of a password manager that will store login credentials is useful. These solutions allow you to create very strong passwords without being required to remember them. Some operating systems, such as later versions of Mac OS X, as well as some web browsers, have built-in password management capabilities, but there are numerous commercial packages available, as well.

Edition: 4.2116

References

1 http://www.privacyrights.org/data-breach
2 Completely Automated Public Turing Test to Tell Computers and Humans Apart
3 Source: *Mobile Enterprise Applications and Solutions FutureScape*
4 http://gizmodo.com/the-25-most-popular-passwords-of-2015-were-all-such-id-1753591514

Edition: 4.2116

About ThinkHR

ThinkHR provides expert HR knowledge solutions designed to help people and companies thrive. Combining the best of human expertise and innovative technology, ThinkHR's solutions include the industry's first and most used HR hotline, an award-winning online HR knowledge base, and a comprehensive eLearning platform.

ThinkHR's mission is to give its partners a powerful competitive advantage to help them strengthen their client relationships, manage risk and win more business. Equally important, the company is passionate about empowering HR professionals and other executives to become more efficient, productive and successful.

For more information, visit thinkhr.com

ThinkHR
855.271.1050
contact@thinkhr.com

About Osterman Research

Osterman Research provides timely and accurate market research, cost data, cost models, benchmarking information and other services to technology-based companies. We do this by continually gathering information from IT decision-makers and end-users of information technology through in-depth market research surveys. We analyze and report this information to help companies develop and improve the products and services they offer, and to help organizations make better decisions about their security, archiving and other capabilities.

For more information, visit ostermanresearch.com.

Edition: 4.2116