The Ultimate
IT Handbook
for Employees

MRW
SYSTEMS, INC.
IT Managed Services

www.mrwsystems.com
info@mrwsystems.com
(410) 751.7111

Contents

Welcome

Hello and welcome to MRW Systems' Ultimate IT Handbook for Employees!

I wrote this eBook because technology moves so fast that it's not always easy to keep up with. Technology is consistently evolving, and as a result, there are constant updates to software, hardware, and everything in between.

This annual tech upgrade cycle can create quite a headache for users. It seems like once you get comfortable with new software, the software changes once again.

With the speed of change in technology, it's understandable that not everybody will be at the same comfort level when it comes to actually using it.

I first noticed the growing "I don't even know the basics" dilemma when I founded my IT service company in 1997. There's no driver's ed class for tech. Somehow, users are just supposed to know how to use their new camera, phone, printer, email platforms, and social networks.

But that's easier said than done.

The point of this eBook is to share essential technology tips to make your user experience with technology faster and easier.

Inside the eBook, you will find an array of helpful tech information, like how to create strong passwords and what to do if you accidentally deleted an important file.

There are tips, tricks, and even, pop quizzes.

Enjoy!
Michael Wolinski
CEO, MRW Systems

Why Trust MRW Systems?

We've been there and done that.

MRW Systems is a managed IT service provider for small to medium size business. We are one of the country's leading MSPs with over 20 years' experience. We tailor our services to our clients because we believe there is no one-size fits all solution with technology.

We work with our clients to help them achieve their business goals. Their success is our success.

"We've been a client of MRW since 2008, and WE have no internal IT services department. In 2012, we were purchased by a much larger organization with a fairly substantial IT department. Despite this, we have remained a client of MRW's IT Services. We valued the input from MRW during the transition period, and recently we've signed a new contract with MRW, so they can continue to support us. It's been a great partnership." –Eileen

"Michael, very nice job on the overview of the status of our systems and security… Our company's CEO noted that it was the most informative assessment concerning our company's IT assets that he has ever received. He noted Michael came prepared and had exceeded his expectations. I received votes of confidence from the group for our selection of MRW. MRW's service and the level of review of our IT infrastructure has met my expectations. Please keep up the good work." –William

The Truth about Passwords

“Be sure to use a strong password” is advice we all constantly see online. But what does that actually mean?

In this section, we’ll go over how to create a strong password—and, more importantly, how to remember it via a password manager.

Password Rules to Follow

Passwords are the most critical components of using the internet today, but they also can be a vulnerability to your security. How well will your passwords stand up to hackers? Will your passwords defend your data? Here are 9 rules to follow to create a bulletproof password:

1

Don't tell your password to anyone!

Nobody should ask for your passwords, and you should never give your passwords to anyone. We recommend that you only give your password to a trusted and verified tech support person. After that tech person finishes fixing your IT problem, you should change your password immediately.

2

Use unique passwords

Never pick a password that is a name or your pet's name, even if it's in a different language. You should also avoid easy to guess numbers, such as your age, zip code, yours or a family member's birthday, or anniversary.

3

Mix-up capitals

Don't use obvious placements for your capitals. Instead try something like this "k(wVEw47!oLyn21" or "tQhAM31DH5tB!SFx".

4

Use long passwords

Use passwords that are at least 15 characters long. I know that sounds like a lot, but it'll help you stay more secure. Also, we recommend that you never write down your passwords.

5

Don't use the same password

This is a hard one, but worth the extra effort. You should use a different password for each website. And try to avoid using simple patterns like "amazon4me", "netflix4me" for different sites because those are too easy to guess.

6

Change your passwords

For example, you should change your online banking password every 60-90 days.

7

Make your security question a password

Sometimes websites ask you to enter an answer for a "security question" in case you forget your password. Instead of answering the question, use a hard to guess password.

8

Use extra security features

Say yes to dual authenticators! If your bank or webmail offers you these extra security features, use them.

9

Password procedures

Use the password procedures your company requires. At home consider using a password manager such as KeePass, PasswordSafe, or LastPass to name a few. Password managers make your internet use a lot safer and easier.

MRW SYSTEMS, INC.
IT Managed Services

Pop Quiz: Passwords

Let's test your password skills! Below, you'll find a series of questions about the information you just read. You'll find the answers on the next page in the lower right hand corner.

1. Ideally, what characters should you use in a password to make it strong?

a. Letters and numbers

b. Mixed case characters

c. Special characters

d. All of the above

2. How long should a strong password be?

a. 8 Characters

b. 15 Characters

c. 5 Characters

d. It doesn't matter

3. Is the following statement true or false? I have a really strong password, so I should be able to use it for years.

a. True

b. False

4. When it's time to change your password, what's the best way to choose a new one?

a. Add a number or special character to the end of your old password

b. Pick something easy to remember such as a football team or your birthday

c. Choose something quick and easy to type in so nobody can see it

d. Choose something you can remember, but modify it with a complex pattern that only you know

5. Strong passwords can be difficult to remember, what can you do to avoid forgetting them?

a. Use mnemonics (acronyms or phrases)

b. Develop a password strategy

c. Use password management software with encryption

d. All of the above

Email Tips

Security & Beyond

Email is by far the number 1 way networks are compromised. In this section, we'll go over some simple yet important security tips you should know in order to keep your email account as secure as possible.

And since we're talking email, I'll also share some tips and tricks on how to manage your inbox and keep it from becoming a disaster zone.

Password Pop Quiz Answers: D, B, B, D, D

How to tell if an Email is Fake

Can you spot a fake email? Phishing is the fraudulent practice of sending bogus emails claiming to be from a reputable company in order to trick individuals to reveal personal information like passwords and credit card numbers.

Here are 5 tips on how to identify phishing or fake emails:

1 Sender's Email Address

The first question you should be asking yourself is does the email address look fishy. For example, let's say you get an email saying it is from Your Bank, but the email address is strange. The address is YourBank@hotmail.com. That should be a red flag. The sender's email, especially from a bank, should not be using a public account, like Hotmail, Gmail, Yahoo, etc.

2 Incorrect URLs

Hackers use fake sites to steal your information. Watch to make sure the URL is actually the one you want to be going to. How do you find that out? If you're on a computer, hover your mouse over the link to see a preview of the link in the status bar. The status bar is located at the bottom left-hand corner.

For example, if you think the URL should be taking you to Target.com, but when you hover over the URL you see target.com.123.nl in the status bar, you should not follow that link.

3 Nosy Requests

Legitimate banks and most other companies will never ask for personal credentials, like PINs and card information, via email. You should be suspicious of all emails and websites requesting your Social Security number, identification number, or any other sensitive information.

4 Your Name

Does the email in question use your name? Illegitimate and fake emails will often address the receiver as a "valued customer" or "to whomever this may concern". Also, if your name is spelt incorrectly proceed with caution. Remember if this email is real that person or company should have your correct information on file.

5 Typos

Real businesses are serious about email. Legitimate messages usually do not have major spelling mistakes or poor grammar. Read your emails carefully, if something seems off, don't click on anything.

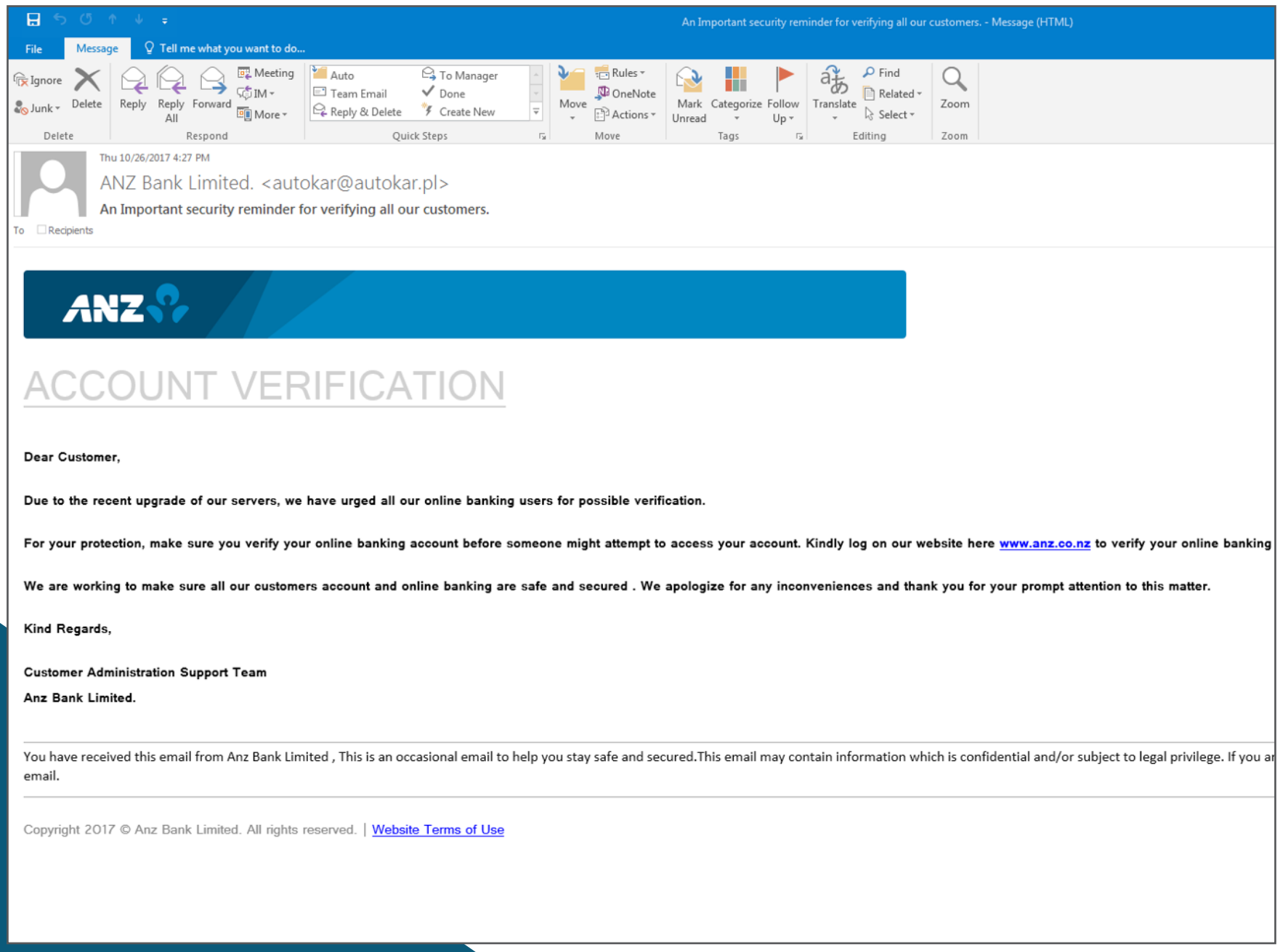
Pop Quiz: Phishing Emails

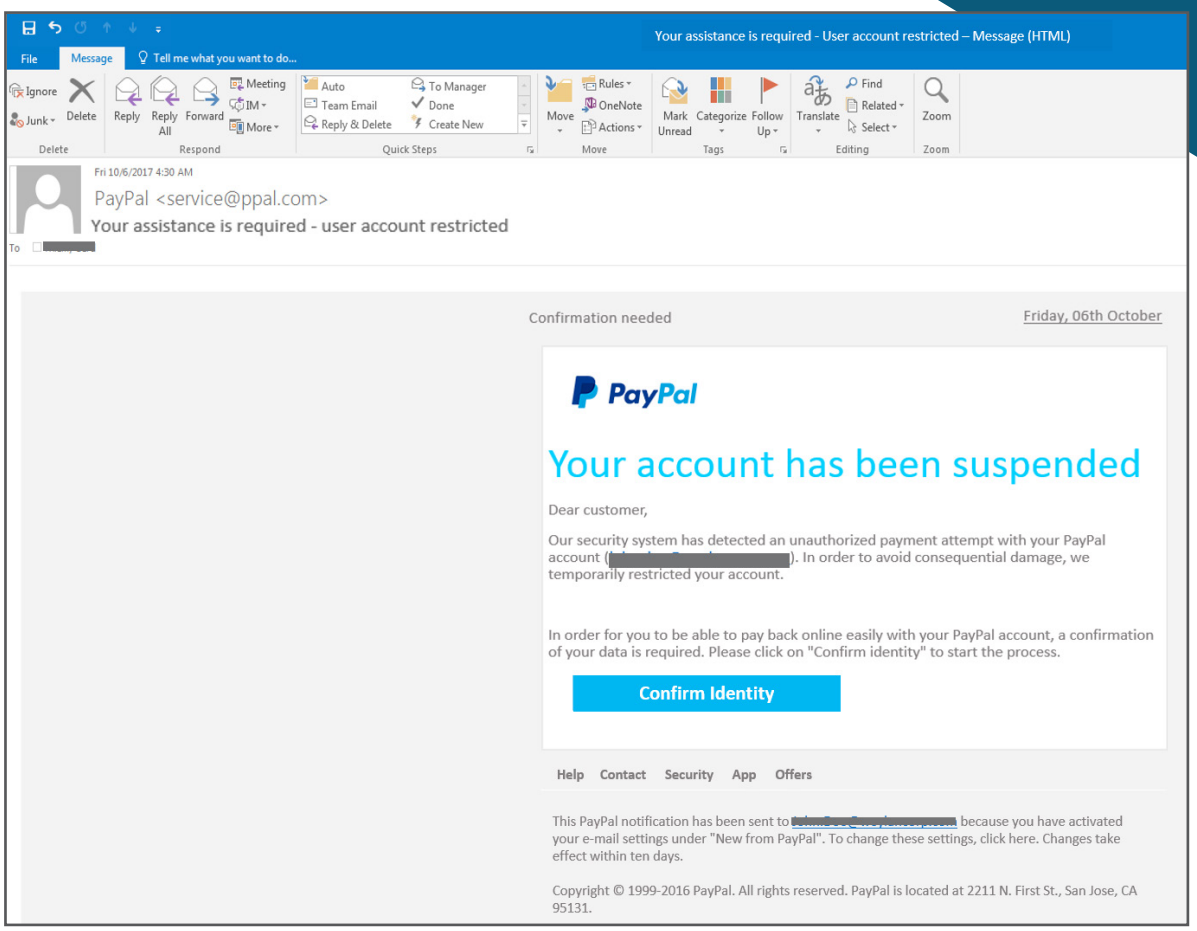
Ready to defend yourself against phishing attacks? Let's find out! Below, you'll find a series of questions. You'll find the answers on the next page after the quiz in the lower right hand corner.

1. Is this email legitimate or not?

    a. Legitimate

    b. Phishing

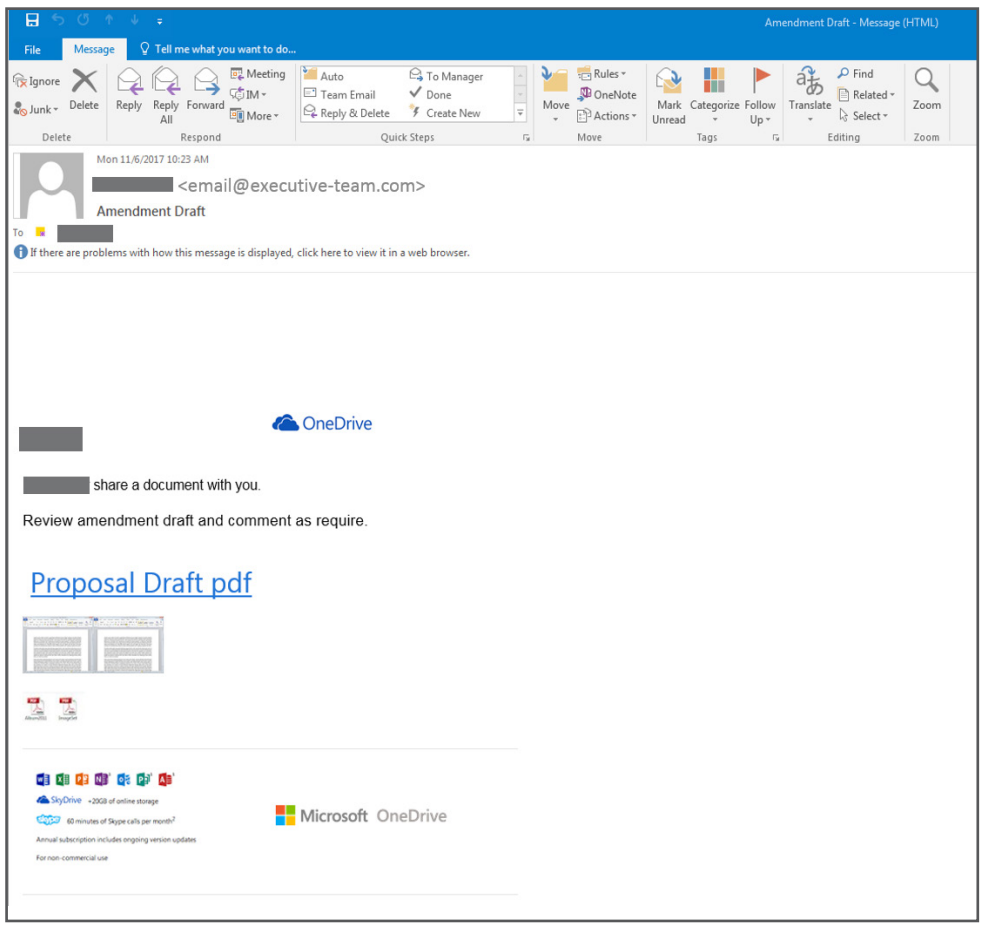




2. Is this email legitimate or not?

a. Legitimate

b. Phishing



3. Is this email legitimate or not?

a. Legitimate

b. Phishing

Messy Inbox?

Today's corporate world is bombarded with dozens of emails every day. For many of us, the sheer amount of emails we receive leads to an unruly inbox that hides our important emails and eats away at our productivity.

If you're ready to change your habit with email, here are a couple helpful tips.

But before you even think about touching your inbox make sure you understand your company's email policy. Most businesses do not want their employees to delete emails, instead they encourage employees to archive emails.

Unsubscribe
It goes without saying, the first thing you must do for a tidier inbox is get rid of unwanted emails. Go through your inbox and unsubscribe from any and all email notification sources that are not important to your day to day operations. Most emails will have an unsubscribe button or link in the bottom of the email.

Organize by Folders or Labels
Creating folders (or labels) within your inbox can help you categorize the various types of emails you receive on a daily basis. Focus on creating folders based around the various roles you assume during your job, so that you can more easily sort your mail according to the different tasks you perform

Touch it Once
This is a mindset you have to work hard to get into, but it's a good habit to have. When you open a message, review it and then do something with it. Don't let it just sit there! Emails that sit in your inbox will have to be weeded out eventually, so why wait.

Understand and Use EOM
EOM means "End of Message" and is a handy time-saving tool. Basically, EOM can be inserted at the end of email subject line to indicate there's nothing in the message. It basically means there's no need to open this email or reply back. What you read there in the subject line was all the sender needed to say.

Phishing Pop Quiz Answers: B, B, B

Oh no! I deleted an Important Email!

Don't panic! There might be a solution available to you.

If you have accidentally deleted an email, your email host might have a copy of your emails.

OUTLOOK

When you delete an email message, contact, calendar item, or task, it's moved to the "Deleted Items" folder in your mailbox.

If the item is still in your Deleted Items Folder:

1. In your email folder list, select Deleted Items
2. Right-click the item and then select Move > Item

If the item is no longer in your Deleted Items Folder:

1. In the Left pane of Outlook.Office.com, select the Deleted Items Folder
2. At the top of the window, select Recover Deleted Items
3. Choose the items you want to recover, and select Recover > OK

GMAIL

If Gmail has not deleted the messages from the server, you can recover deleted emails from your trash folder.

1. Open your Gmail
2. Click the drop-down arrow on the search box located at the top of the screen.
3. Fill out the form with the missing email's information
4. Click on the blue search button

If your emails are deleted from the actual server, Gmail (the free version) is unable to restore them for you. However, if you are a Google Apps user, they do offer a solution.

If you delete an email and it stays in the trash for over 30 days, the email will be permanently deleted from the trash.

If all else fails, contact your IT service provider–there's a good chance that they will be able to restore your deleted email through data backups.

How to become a **Firewall**

As an employee, you are an important line of defense against threats to your company. In this section, we'll go over ways you can stop hackers from accessing important company data.

Essentially, you will learn how to become a human firewall.

How to Become a Human Firewall

A firewall is the first line of defense against intruders and a critical element to any modern-day business.

Often when talking about firewalls, we only think about the technical ones–the firewalls the IT guys handle. But did you know that as an employee you can act as a firewall to keep you and your company safe?

As an employee you are an important line of defense against threats to your company. You are responsible for understanding your organization's policies around Internet browsing, email, and device usage with every employee on a quarterly basis.

As such, you should be actively involved in protecting your organization's most critical assets, your company data.

No More Paper Trails

Look around your office or cubicle, do you have any scraps of paper with passwords on it? Client files laying around?

These paper trails can be very risky exposure points for your organization. Even if your office doesn't see a lot of foot traffic, there are always some visitors or ancillary staff.

I strongly recommend you keep a tidy desk and make sure you understand your company's policies around paper in the office.

Lock Your Computer

Leaving a computer running unattended is a bad habit. We recommend that all employees lock their computers when they leave their desk for a meeting or lunch.

Unlike logging out, a locked computer doesn't shut down everything.

Once a computer is locked, no one can access it unless they have the computer's login information. However, at the end of the day, it is important that all employees log completely off their computer.

Here's how to lock your computer on Windows:

• Press the Windows key+L key combination on the keyboard
• Or, click the padlock button in the lower-right corner of the Start menu

And with OS X:

• Press Control+Shift+Power on the keyboard. If you are using an older Mac use Control+Shift+Eject instead
• Or, click on the Apple icon in the top left corner of your screen, and go to "Lock Screen"

Please note, on OS X, make sure the "Require password after sleep or screen saver begins" is turned on. You can do this through System Preferences > Security & Privacy > General.

As soon as you press those shortcut keys or click the padlock, the initial login screen appears; no one can access the computer at that point unless they have the computer's login information.

When was your Last **Update?**

You're hard at work on your computer and a message suddenly pops up saying, "a software update is available". You're busy, so you click "cancel" instead of "install", thinking you'll get to it later, but you never do. Sound familiar?

Not updating is a bad habit to get into! In this section, we'll go over why you should stop putting off these updates.

When was Your Last Update?

And Why You Should Stop Putting Them Off...

Why are software updates so important? The main reason is because the majority of malware out there doesn't exactly target new and unknown security vulnerabilities. Instead, it goes for well-known exploits that have already been fixed in the latest version in the hopes that companies haven't updated.

What's important is that despite all the pain, updating is usually well worth it. As it allows you to prevent very costly breaches and leaks and helps keep sensitive data protected.

Here's a of couple tricks on how to find out if you have the latest updates:

WINDOWS 10

Windows 10 periodically checks for updates, so you don't have to. When an update is available, it's automatically downloaded and installed. But if for whatever reason, you think you may have opted out of an update, select the Start > Settings > Update & Security > Windows Update > Check for Updates.

Also, Windows 10 currently keeps a history of successful or failed updates. You can find it by opening Start > Settings > Updates & Security > Windows Update > Update History.

MAC

When a new major version of OS X is released, you can download the upgrade for free from the App Store. Click the Apple menu and select "App Store". Then, click the "Updates" tab on the top of the App Store window. Finally, click "Update" next to any available updates to install it.

If you are still unsure if you have the latest software updates, please contact your IT person.

Conclusion

You've made it through the MRW Systems' Ultimate IT handbook for Employees. I hope you learned a new trick or two.

Using these tips and tricks on a daily basis will certainly make your time on computers more enjoyable, practical, and secure.

If you are ever looking for more IT information, please feel free to check out MRW Systems Blog at www.mrwsystems.com/blog.

The MRW Systems blog offers readers the latest IT news. Key topics include tech tips, product reviews, cyber security news, and software & hardware news.

If you have any feedback about this eBook, don't be afraid to reach out to me directly.

My email is michaelw@mrwsystems.com.

www.mrwsystems.com
info@mrwsystems.com
(410) 751.7111