**End User Training**

We have partnered with your ORGANIZATION to offer you all a tool both for professional and personal use, called LastPass, which is a password management application.

**What is a LastPass?**

We serve as a rolodex of your passwords, so as you go throughout your day on the internet, we're just there in the background filling in your usernames and passwords for you.

A primary benefit of this is that you can stop reusing passwords - so when a site gets compromised and they obtain a password with your date of birth and the name of your first born child, they're not able to access multiple sites with the same username and password.

What LastPass can do for you, is generate (and remember) long, extremely complex passwords that are great at keeping you secure online. We encrypt all of your data locally, only. Which means that your master password and your data is yours and yours only and at no point are we able to see into this data. It is important to remember only one password moving forward, your master password.

**Values of LastPass**

It's simple: No more writing down passwords of sticky notes or within spreadsheets. (Like my mom who stores important passwords and items like my dad's SSN as a contact in her cell phone?!)

Security: LastPass protects your data at every step and allows you to generate passwords that are incredibly hard to crack. If someone was able to get ahold of your vault, if you got a virus on your machine, they just got a blob of encrypted data with military and bank level encryption that would take them years to determine what they obtained.

Convenience: You just go about your day and we exist in the background helping you along the way.

**Creating your account**

This first thing that happens, is that you'll receive an email invitation with a link to create your strong master password. It is to be unique, please do not use your AD password.

**Explore your extension**

You'll add a browser extension to assist you in capturing your credentials, accessing your vault and generally helping you throughout your day.

**In-field icon**

You'll also see an infield icon, that as you browse, LastPass knows when to help you and gives you quick access to your passwords directly on the webpage.

**Mobile**

LastPass syncs to multiple devices, so you're able to have it where ever you need it. Multiple browsers, phones, tablets etc.

**Passwords on autopilot**

Autosave & autofill - as you log into websites, LastPass will offer to remember the credentials for you. Select yes and when you return the next time it will auto fill those saved credentials for you and you just need to select sign in.

**Password Generator** - As you create an account for a site, you can generate a complex password the first time. When you're creating a new account, there will be a password generator icon - selecting that you can generate a completely unique password that you'll never need to remember.

**Form fill** - All your personal data you would normally fill into a site. As you create accounts or make purchases, it will fill in the available information for you, including credit card information which is much more secure than storing your credit card information on the site itself. For example, I prefer to online shop but I don't want to store my card information on a plethora of sites. Instead, I'm able to securely store my card information and still have the ease of quickly checking out using LastPass.

**Secure Notes & Attachments** - It's a note that you can use to save information that you would like secured. Such as SSN, WiFi passwords, insurance information and just general notes (Christmas list anyone?)

**Security Challenge** - Quick and easy way to audit your passwords for weak, duplicate, old and potentially breached passwords; so you can see how secure your online footprint is

**Shared Folders** - Create a shared folder. For example, the Social Media team within the company. There are multiple accounts and several people should have the ability to access. You can securely share those credentials with the team, allowing the password itself to be complex and it is contained within the vault securely.

**Linked Personal Account** - Keep work and personal accounts separate and safe. What is in your personal account is only available to you.

**Demo**

**LastPass 101**

1.      Start with invitation

2.      Prompted to set up multi-factor

3.      LastPass Extension and Vault - (Tutorial) *We do not suggest using the Importer option, instead we recommend that you build your vault as you log into sites naturally. It could pull old or random passwords saved in your computer, such as the WiFi password from a hotel you stayed at once.*

4.      How to Save a Site

a.      Go to Amazon and login and save demo login information

b.      LastPass will automatically try to determine what folder the login belongs in or create a new folder. By selecting "edit" and change or create a new folder.

c.      You can also select "never remember"

d.      Logout to show that the username/password is pre-populated - the "1" indicates that there is one set of credentials saved to this URL. If you had multiple you could choose which set you'd like to login with

5.      Move back to the vault showing the extension (all of these quick links are available in the vault as well)

a.      Left side tool bar

b.      Icon toggling

c.      Searching

d.      Sites

                                i.          Add items \*we do recommend savings as you navigate the web

e.      Edit site

                                i.          Top 100 sites - you have the option of auto changing the password to something unique and secure

                               ii.          Notes -security questions

                              iii.          Advanced Settings

1.      Autologin -only use this if you have only one set of credentials for the site, if you have multiple it will not allow you to choose which one you'd like to use

6.      Add a Secure Note

7.      Add Form Fill

a.      Name + Email address

8.      Go to LinkedIn.com to create an account using the form fields

9.      Sharing Center -> I'm part of a team that uses shared logins for certain accounts and I would like to be able to share the passwords with my team

a.      Create a new shared folder

b.      Now the folder exits

c.      Manage -> invite users

d.      To add sites to the folder - navigate back to your vault and add something to the shared folder

e.      Easily convert a folder to a shared folder from your vault

10.   Security Challenge  \*Make sure you have a site that is not shared\*

a.      Confirms your password to decrypt locally

11.   Linked Personal Account \* if applicable

12.   Account Settings

a.      Change Master Password

b.      The remaining features are managed by your administrator

13.   More Options

a.      Deleted Items

                                i.          Can restore

b.      Help Section

                                i.          Users Manual - very robust

                               ii.          Tutorials & Videos

14.   Q&A