OnDeck

TOP 7 UPCOMING SECURITY IMPROVEMENTS FOR ONDECKERS

Stop Hackers from Getting In

1. Better Passwords
2. Stronger VPN Access
3. Secure Internet Browsing

FLIP ME !

Key Dates

FEBRUARY

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29					

Sensitive Data Visibility & Control — 1

Encrypted Email — 3

Better Passwords — 10

Strong VPN Access — 15

Laptop Encryption — 25

MARCH

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Secure Browsing
USB Drive Blocking — 1

#1 Better Passwords

I make **GOOD** passwords and have to change my password **LESS** frequently.

Any new passwords created after Feb 10 meet higher standards.

THEN	NOW
8 characters long	**12** characters long
Change every **90** days	Change every **180** days

YAY!

#2 Strong VPN Access

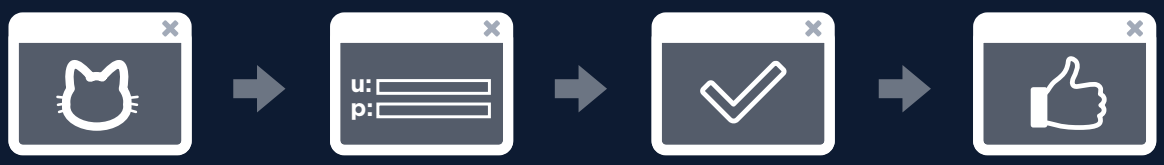
Mandatory Passcode and Password-based VPN (known as "Two-factor Authentication (2FA)" enrollment is **Feb 4-12**. All VPN access requires passcodes beginning **Feb 15**.

20% OF US GAVE OUT OUR PASSWORDS IN THE LAST SECURITY PHISHING TEST.

I use **PASSCODES** to access VPN with my password.
I **TAKE** my laptop home when I work from home.

#3 Secure Browsing

*I LOG IN to use the Internet because it **PROTECTS** me from the* DARK SIDE.



1. Look for cats
2. Login
3. Pick Zscaler Secure Browsing
4. DONE & PROTECTED!!!

Mandatory internet logins beginning **March 1**. It only asks you to log in once in a blue moon.

Stop Hackers from Leaving with the Goods

4. Laptop Encryption
5. USB Drive Blocking
6. Encrypted Email
7. Sensitive Data Visibility and Control

OnDeck

WHY?

We have very **sensitive** customer information. We must protect customer identities and our reputation. Our partners demand it and our customers expect it.

Thanks,
The Management

#4 Laptop Encryption

I **HELP** Technology **ENCRYPT** my laptop so if my laptop is lost/stolen I don't cause a data breach.

Mandatory laptop encryption is happening right now, department-by-department! Please leave your laptops when we ask you to. The first encryption is very manually intensive.

IF I LOSE MY UNENCRYPTED LAPTOP, EVEN WITH A PASSWORD ALL DATA CAN BE STOLEN.

#5 USB Drives are Blocked

I **DON'T USE USB** keys or drives because they can bring malware or, when lost, cause data loss.

*Mandatory USB key/drive blocking beginning **March 1.***

Do you use USB keys/drives for backup?

Use your personal Microsoft OneDrive instead. It's like Dropbox.

https://ondeck-my.sharepoint.com/

#6 Encrypted Email

I **ENCRYPT** email containing sensitive information to third parties.

*You may encrypt email you send to people outside OnDeck beginning **Feb 3.***

For a complete guide: **https://goo.gl/8uRFO2**

How to Send Encrypted Email

1. Write your email

2. Add [SecureMessage] to subject line. SEND!

#7 Sensitive Data Visibility & Control

Data Loss Prevention software helps OnDeck understand where sensitive customer information is in the company and how it is used so we can enable more protective measures against accidental or malicious data breaches. Rollout begins **Feb 1** to employees with access to certain business partner data.

*My laptop **ALERTS** Security when I send sensitive information outside OnDeck.*