3/8/19

landF/X

Top 10 Security and Password Tips for Small Business

WEBINARS

Forrestt Williams

Land F/X for 6 years:
Tech Support, Office IT, Graphic Design,
Website Design, Maintenance, & Development,
Video Editing, and much, much more.

support@landfx.com

Outline

1. VPN
2. Multi-Factor Auth
3. Password Managers
4. Simple Password Guidelines
5. Phishing
6. Audits
7. Backup your data!
8. Purge the old
9. Install those Updates
10. Firewall, Virus, and Malware

Why is security important?

- You could have your **bank account cleaned out.**
- You could have your **identity stolen.**
- You could have your **website hacked.**

You all saw these headlines in the news repeatedly in 2018.

We want to break down some of these intimidating security concepts and best practices for you, our Land F/X clients.

1.
Use a VPN

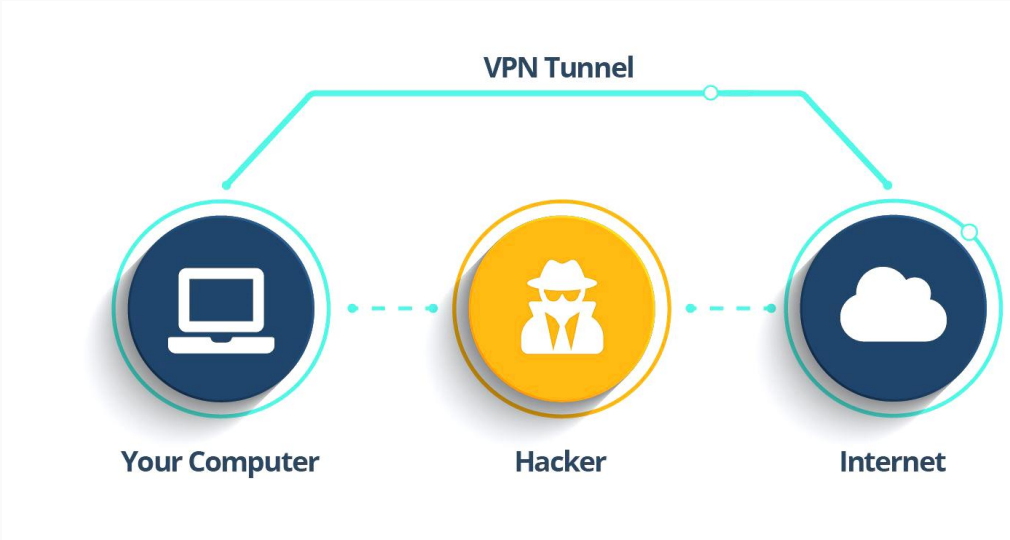
What the heck is a VPN
and why do I need it?

Virtual Private Network

It's easy to 'listen' to internet traffic on a public WiFi. Every time you login to a website on public WiFi your username and password can be stolen.

A **Virtual Private Network** uses additional encryption to mask your internet traffic.

At a coffee shop or hotel lobby? **ALWAYS Use a VPN!**



Virtual **P**rivate **N**etwork

There are several highly rated and affordable VPN services on the market, here are just a few. Choose what's right for you:

Several of us in the Land F/X office have experience with both **Private Internet Access** and **Hide My Ass**. Both of those are secure, affordable, reliable, & most importantly, **super easy** to use.

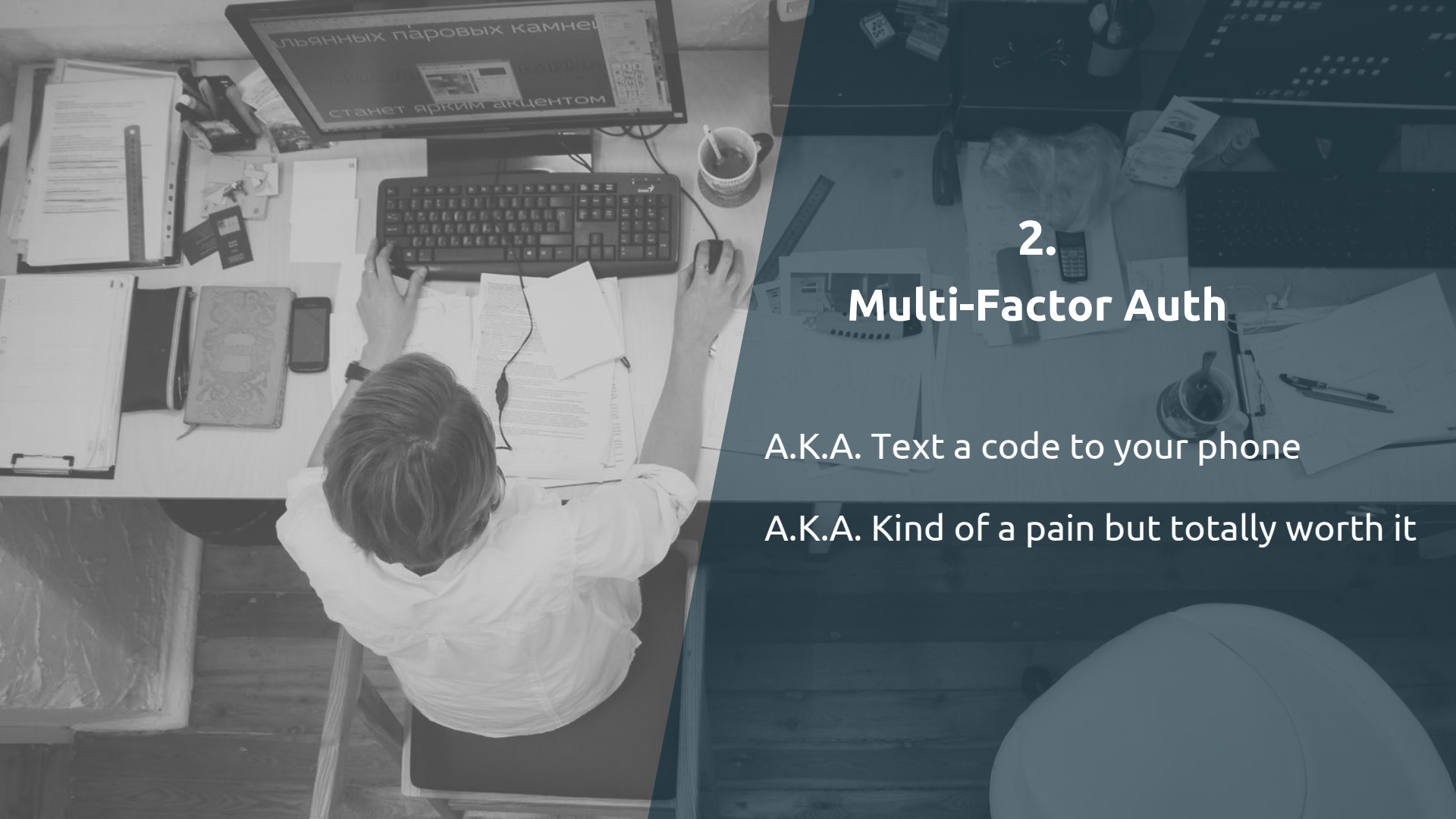
Virtual **P**rivate **N**etwork

Public Wifi Rules of Thumb:

1. **Always use a VPN** when using public WiFi.

2. Make sure no one is **Shoulder Surfing** - AKA looking over your shoulder to see you enter your passwords.

3. If you want extra, super security, don't use the WiFi! Use your cell phone connection instead.



2.
Multi-Factor Auth

A.K.A. Text a code to your phone

A.K.A. Kind of a pain but totally worth it

Multi-Factor Authentication

You know the thing, ‘We’ve sent you a text message with a secret code to prove it’s you.’

Most major companies offer this now, especially in the financial field or major tech.

Multi-Factor Authentication

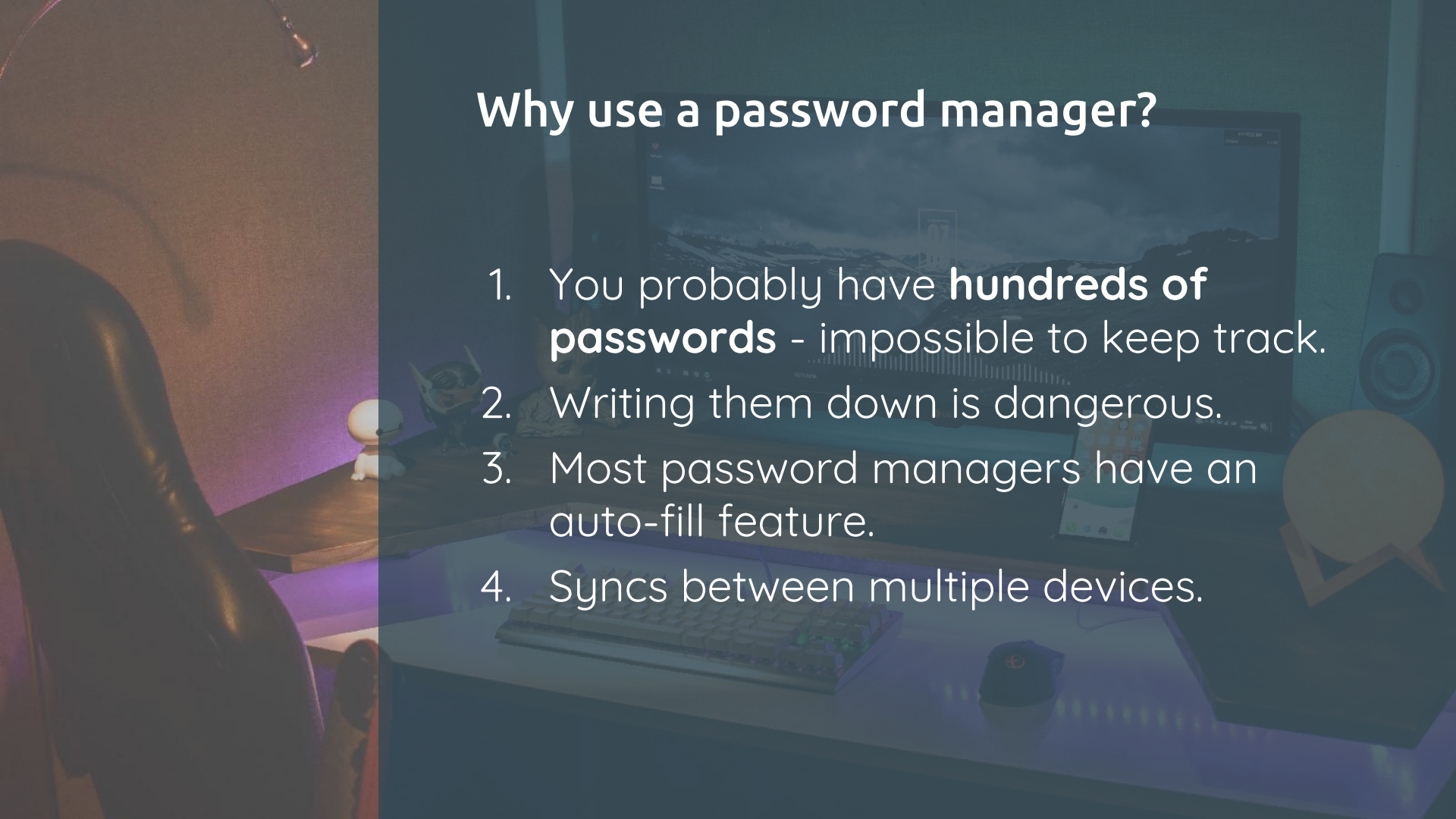
NOTE:
Multi-Factor Auth is only triggered when logging into a **NEW** device.

You might get messages from companies giving you a login code - even if you **didn't login to a new device** - that is hackers or bots trying to login to your account!

If you **DON'T** have this enabled for your sensitive logins, like your bank, Google, Facebook, Microsoft, Amazon, etc - then **you are at risk.**

3. Password Managers

Don’t forget those crazy passwords you come up with!



Why use a password manager?

1. You probably have **hundreds of passwords** - impossible to keep track.
2. Writing them down is dangerous.
3. Most password managers have an auto-fill feature.
4. Syncs between multiple devices.

Password Managers

There are several on the market, here's a few of the most popular ones:

LastPass ****

Pro Account: $36 / year

dashlane

Premium Account: $60 / year

keeper

Business Account: $30 / year

1Password

5 User Business Account: $240 / year

1 User Personal Account: $36 / year

Password Managers

Here's a fun exercise, go to:

https://haveibeenpwned.com

Enter your email to **see how many times your accounts have been hacked!**

This should be a reality check.

⚠ **Never reuse the same password!**

4.

Simple Password Guidelines for secure passwords

Let’s make it easy!

5 Password Rules of thumb

1. **Never write** your password on a sticky note fixed to your monitor
2. **Never reuse** passwords for different logins
3. **Longer passwords** = better security
4. If you can use **autofill** for the login, use complex passwords
   a. Autogenerated, saved, and auto-filled by your password manager
5. If you have to type your password manually (wifi, password manager, etc) use a **passphrase** instead of a password.

Unspoken rule: Don’t email/text your passwords to other people, ever!

Passphrases made easy

A “Passphrase” is a long password made of multiple words, like:

`thispasswordisInsecure` ← This is a silly example, and not secure. Do not use this!

These can sometimes be hard to remember, or hard to type, so we need to find **the right balance between**:

Security

Ease of Typing

Memorable

Passphrase Style #1: Lyrics / Lines

Song lyric, book line or movie quote, with additional characters interspersed.

"**Billie Jean is not my lover**" as a password could be:

```
Billy Jean 1982$$$$ is not my lover
```

"**Are you feeling lucky punk?**" as a password could be:

```
areYOUfeelingluckypunk***.44***
```

A computer that can try **one million guesses per second** would take over **5.34 trillion trillion trillion trillion centuries** to guess the Billie Jean password.

Security: ★★★★★

Ease of Type: ★★★

Memorable: ★★★

Passphrase Style #2: Misspelled Rhymey Phrase

Take a few words that rhyme, misspell them, and intersperse them with symbols, uppercase letters, and numbers.
Examples:

`bleezy565&*&TREEZY`

`BISCUIT^^^456^^^triscuit`

A computer that can try **one million guesses per second** would take over **1.28 trillion centuries** to guess the bleezy565&*&TREEZY password.

Security: ★★★★

Ease of Type: ★★

Memorable: ★★★★

Passphrase Style #3: “DICEWARE part 1”

Using a diceware generator create a **5 word phrase**:

```
useable paprika clip cloning gloomy
```

A computer that can try **one million guesses per second** would take over **45 years** to guess this passphrase – IF they use the same word list.

Security: ★★★

Ease of Type: ★★★★★

Memorable: ★★★★

Passphrase Style #3: “DICEWARE part 2”

TO Make it SUPER secure:
Misspell 1 word, and add extra characters and numbers.

Try to adopt a simple rule of thumb to all of your passphrases, something like:
“1st space **symbol**, 2nd word **capitalized,** 2nd space **number,** 4th word **misspelled**”

It would take a supercomputer over **5 hundred million trillion trillion trillion trillion centuries** to crack this passphrase**!**
https://www.rempe.us/diceware/#eff

Security: ★★★★★

Ease of Type: ★★★★

Memorable: ★★

Passphrase Caveats

Diceware caveats:

- Only works if you **use actual dice or online generators**
  - Humans are bad at actual randomness.
  - Google “Diceware Generator”
- If you want serious security use **6 words!**

Don’t be like Kanye: 000000 is not a good password.

Lyric / Line & Rhymey caveats:

- Most common lyrics or famous lines are already in “password dictionaries” that hackers use to crack passwords. To combat this:
  - Always use **characters and/or numbers** within your passphrase. Preferably something relatable and easy to remember.
  - **Misspell** one of the words!

Why???

You might be thinking:

If I enter my password wrong 3 times in a row I'm locked out!

How can a hacker guess my password with their super-computers?

BRUTE FORCE ATTACK

This is usually when a website has been hacked, their login database stolen. Passwords are encrypted, so the hackers have the data offline and can guess as many times as they like.

Yes, you should be concerned!

Data breaches in **2018 alone** + number of accounts compromised:

- Facebook – 29 million
- Google+ — 52.5 million
- Cambridge Analytica — 87 million
- MyHeritage — 92 million
- Ticketfly — 27 million
- T-Mobile — about 2 million
- MyFitnessPal — 150 million
- Quora — 100 million
- Marriott Starwood hotels — 500 million
- Aadhar — 1.1 billion

Passphrase Resources

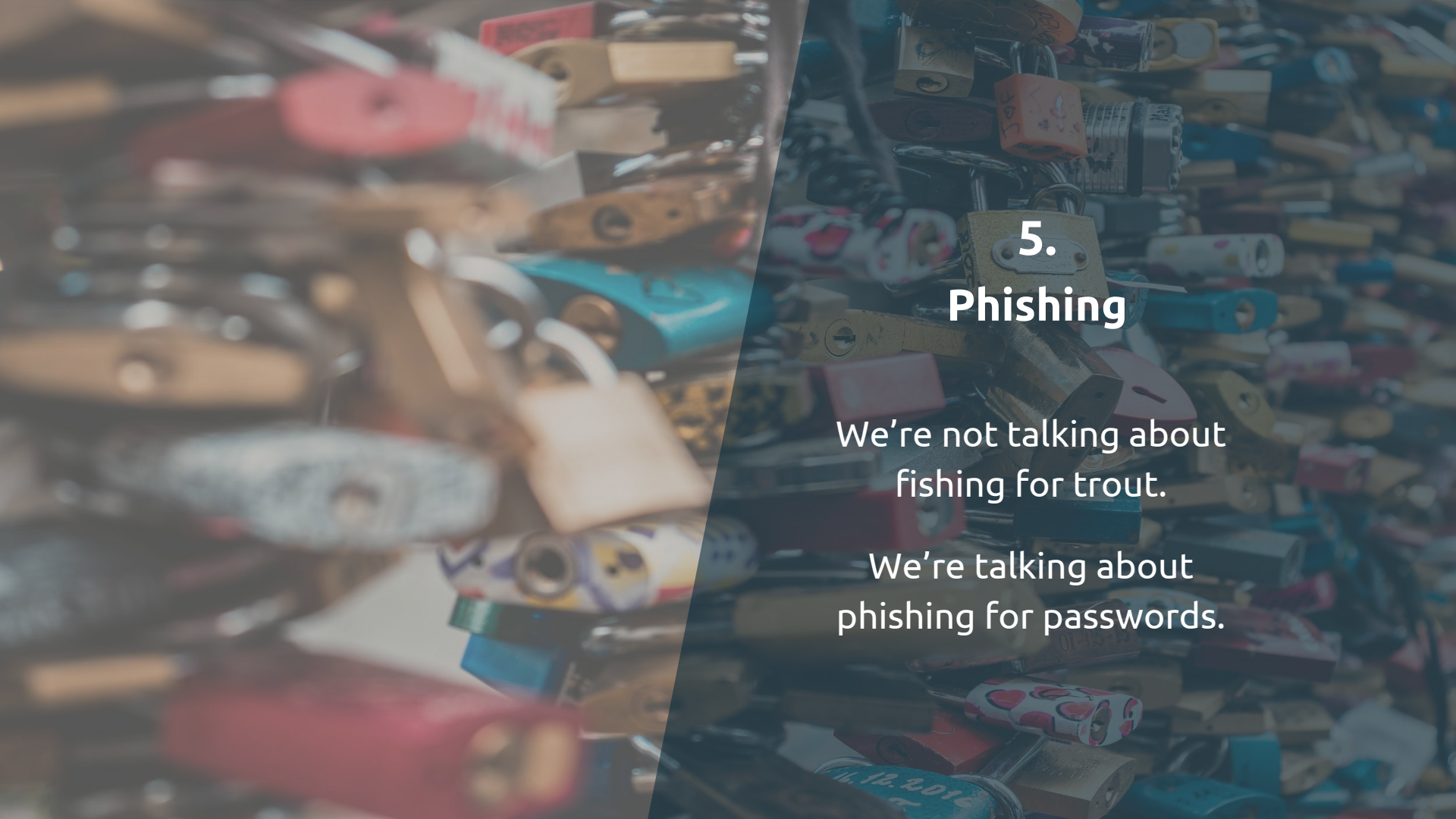
Password crackability estimates*:
https://www.grc.com/haystack.htm?id
https://howsecureismypassword.net/

Diceware Generator:
https://www.rempe.us/diceware/#eff

*Password strength meters should only be used as a rough estimate.

Any of these password styles are acceptable for good security. Choose what works best for you!

Image provided by CORE Landscape
Project created using Land F/X

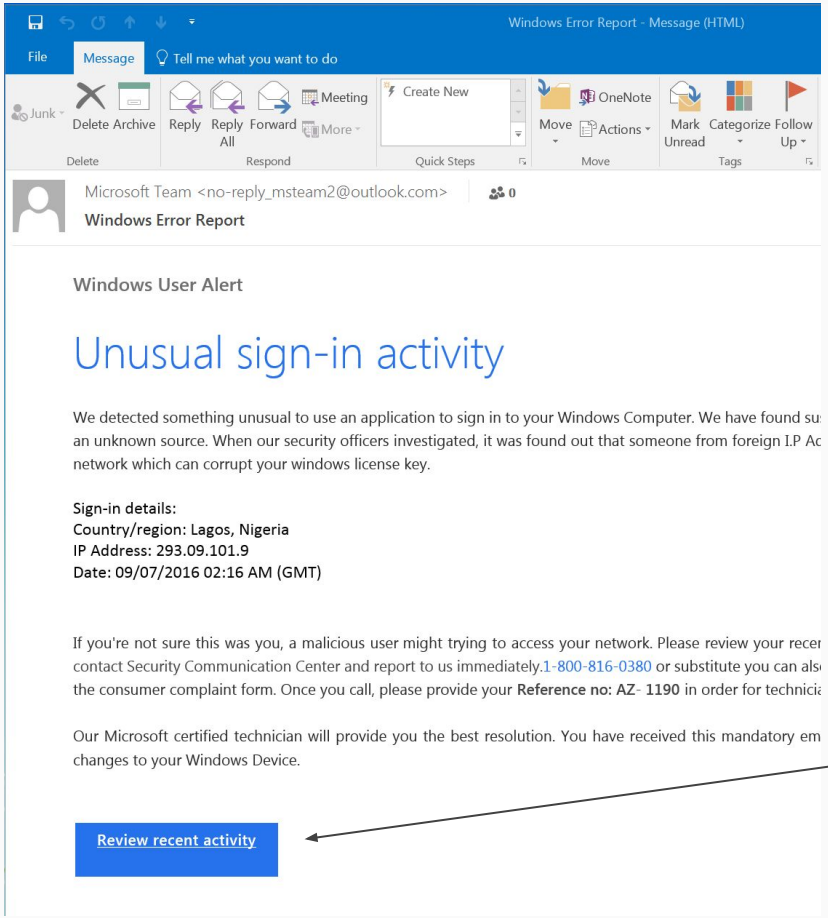


5.
Phishing

We’re not talking about fishing for trout.

We’re talking about phishing for passwords.

What is Phishing?



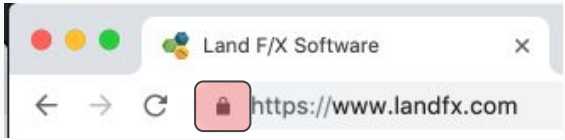
Phishing is when an email looks official, and often contains a login link.

Phishing has gotten **extremely sophisticated**, and is one of the **primary techniques** that hackers can get into your accounts.

This appears legit, but is actually a meta-phishing attack. This link would take you to fake microsoft login

How to avoid Phishing scams?

1. Always **double check the URL** before logging in.
   a. Chrome has a great little **lock** icon to reference:



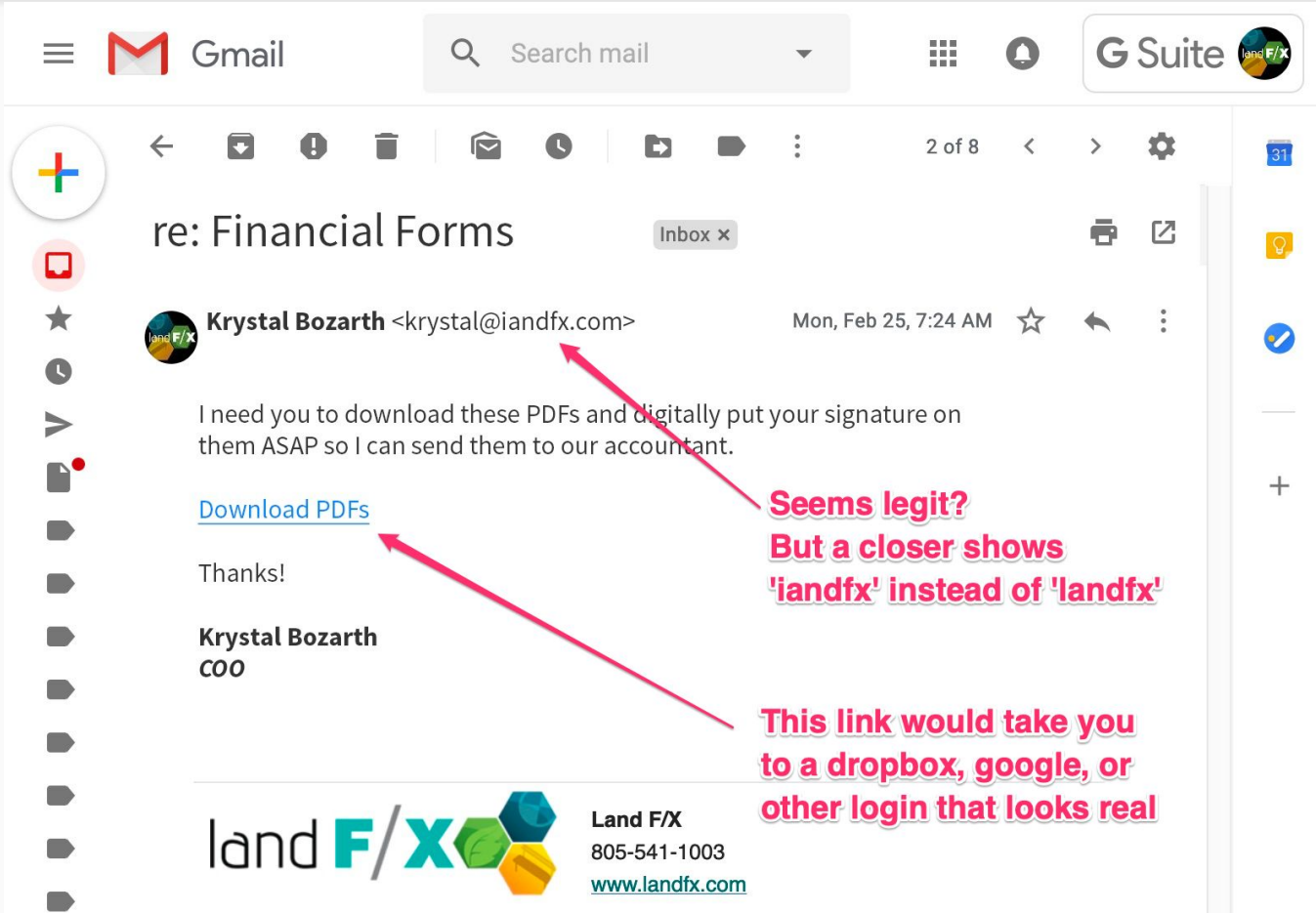
2. Make a habit of NEVER clicking links in emails.
   a. It might seem like a pain but if you never click links you **decrease your chance** of getting phished.

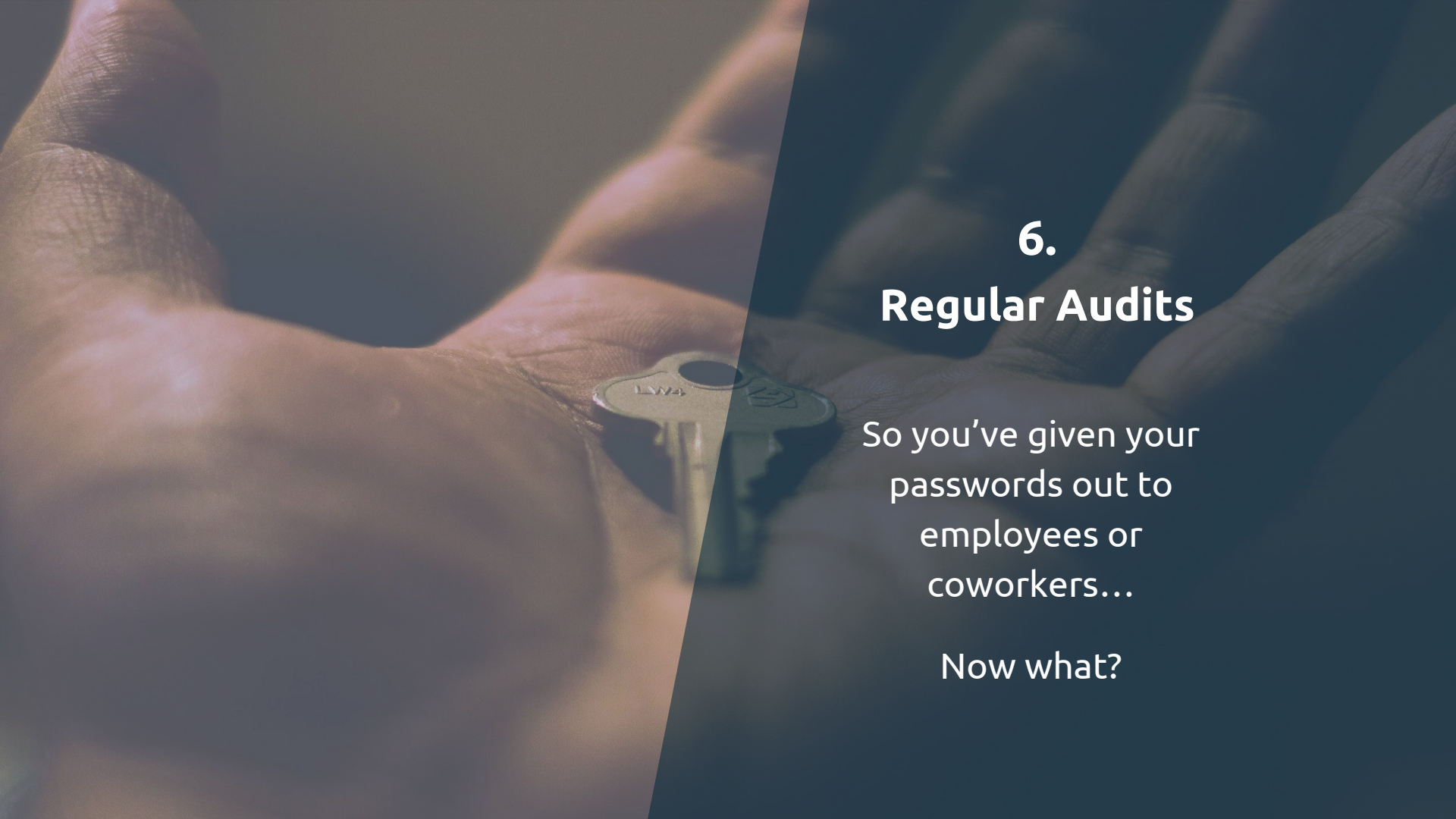
3. Use **common sense** when logging into websites

4. For many services, use your **phone app instead of browser** if you get one of these emails. Then you'll know if the email is legit.

Even internal company emails can be dangerous!

A classic example is a domain that is one letter away from your domain, which, on first glance, looks real:





6.
Regular Audits

So you've given your passwords out to employees or coworkers…

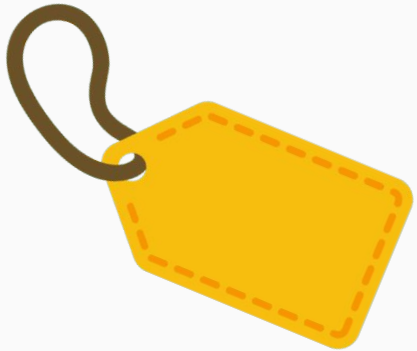
Now what?

Password Audits

- Most password managers have audit features:
  - Scan for password duplicates, password age, etc.

- Use a **tag system** in your password manager every time you share a password
  - “It says here that Bob, who hasn’t worked here in a year, has the password for our Facebook account.
    Time to change that password!”

- Change your sensitive passwords once a year.
  - But don’t use National Change Your Password day, as that’s when internet phishing and spoofing is at record activity!



Ex-Employee Procedure

Let’s say you have an employee or coworker leave the job.

- Do you know which passwords they had access to?
- Do you have to reset ALL your passwords?
  - That sounds tedious and time consuming
- If you had a nice clean tag system in place then you wouldn’t have to change ALL your passwords!

Hopefully you see why this could potentially be a giant security risk!

7.

Backup!!!

Backup!!!

Backup!!!

All this work is useless if you lose it all!

Why Backup

Most common data loss scenarios:

- Fire / Flood
- Drive Failure
- Theft
- Malware

We get around **1 call a week** from clients with severe data loss issues!

It can happen to you!

3-2-1 Backup System

3 - Copies of your data

- System / working copy
- External backup
- Off-site or cloud backup

2 - Different formats

- Internal drive
- External drive or Cloud

1 - Off-site

- Keep offsite backup in a safe or Safety deposit box.

Test your backups quarterly!

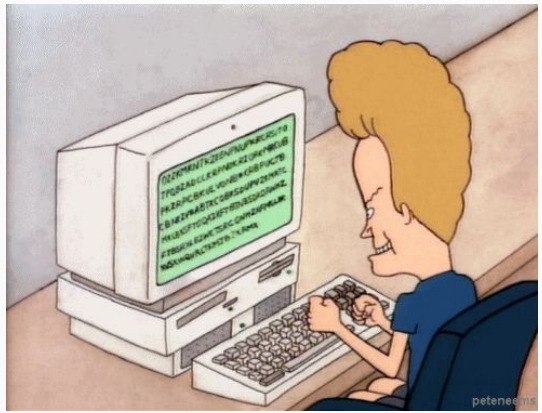
Over the years clients have told us horror stories of losing **tens of thousands of dollars worth of work** because their backup systems didn't function correctly!

Test your backups and restoration procedures

Getting a new computer?

Use this as a good opportunity to **test your restoration procedures**.

- Where is your list of software license keys?
  - Password protected USB drive
  - Password manager
- Where are your backups?
  - And how good are they
- How long is your downtime?
  - Downtime = lost money



- Maybe even pay your IT guy to come in and do a full server restoration
  - Your backups and restoration procedures are worthless if they don't work!

8.
Wipe old drives

Don’t leave your data lying around where anyone can grab it.

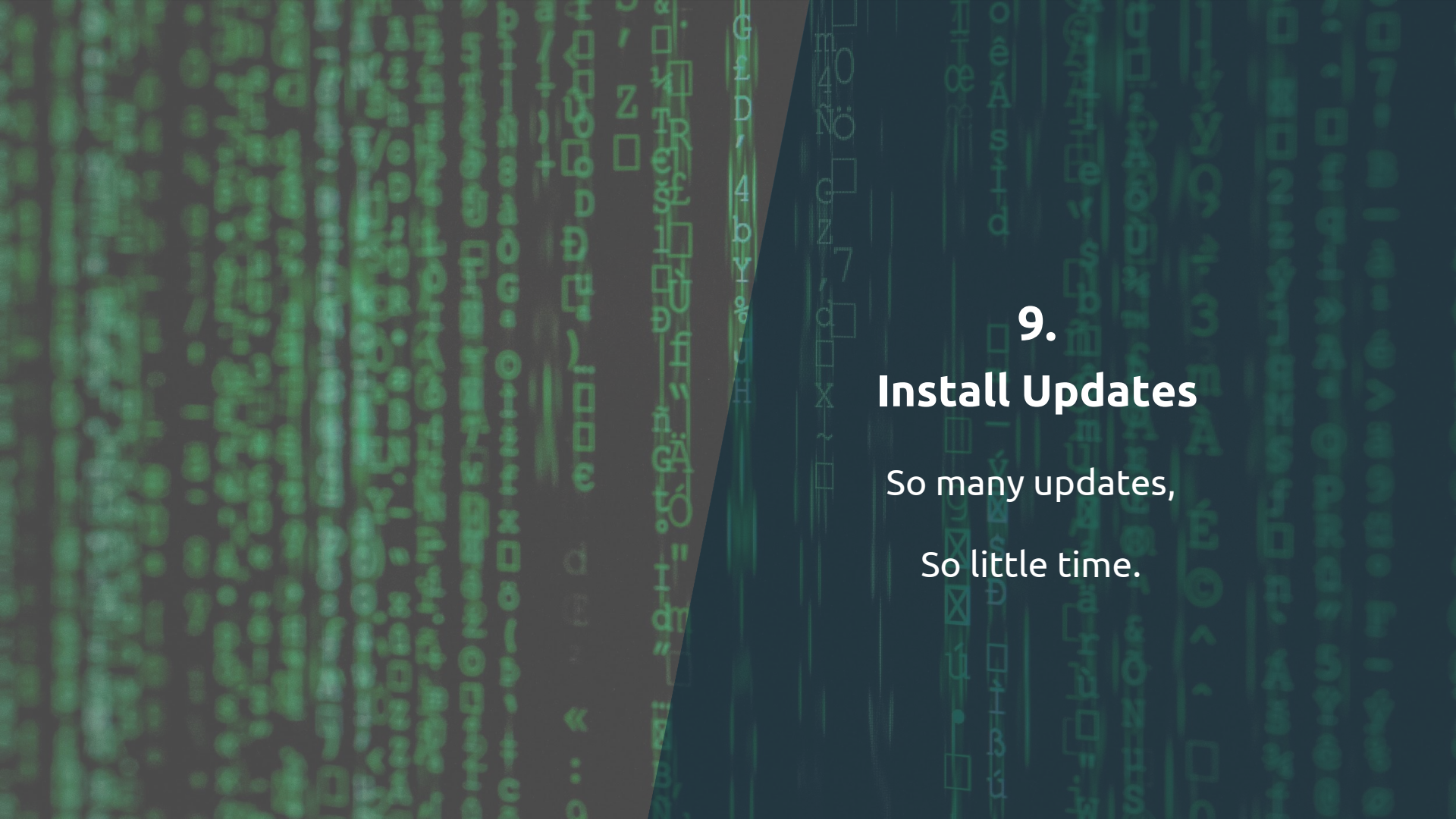
Wipe or Destroy old drives

Having data on old drives can be dangerous!

- Extra USB transfer drives laying around
- Getting rid of an old computer
- Upgrading your Hard drive

Nearly all cities have a mobile paper shredding services that will dispose of your drives safely.

Or take old ‘spinner’ hard drives home and have your kids disassemble them!



9.
Install Updates

So many updates,

So little time.

Updates

Okay, Windows 10 updates are a pain. BUT....

- A majority of software updates are bug fixes and security patches.
- If you don't install the update that mentions security, then you **are** at risk.
- Do yourselves a favor and install the update.

Click 'download' and give yourself a minute.

Step away from your computer.
Go outside for fresh air.
Get a cup of coffee.
Give your computer-soaked eyeballs a rest.

10.
Firewall, Malware & Virus Scanners

A malware scan a day
keeps the Russians at bay.

Firewall

Software firewalls are confusing and tricky.

Instead use your router's built-in firewall!

A "poor man's firewall:"

- Change the default router admin password to a secure passphrase.
  - Some routers will allow you to turn off the web-accessible admin panel.
- Done!

Don't let intruders break in!

Malware & Virus Scanners

There are many great options on the market, but over the years we have consistently recommend Malwarebytes.

- Both Virus & Malware scan
- **Really Easy to use**
- Comprehensive & Regularly Updated threat database
- PC & Mac
- Free version **scans and eliminates malware & viruses!**
- Paid version **prevents infection** @ $40/yr

https://www.malwarebytes.com/

Malware Scanner

Malware can be easy to get from “download sites.”

Stay away from sites such as:

- Cnet.com
- Tucows.com
- Softonic.com

Keep those criminals out!

Wherever possible **only download software through the vendor’s own website** or **official App stores** (Google Play, App Store, etc).

What to do if you've been hacked!

Image provided by YTL
Project created using Land F/X

What to do if you've been hacked

1. **Change passwords**
   a. Run a password audit, ensure that other accounts don't use the same or a similar password
2. **Check Financials**
   a. Change your bank passwords
   b. Keep an eye on accounts. If you suspect your cc was compromised call bank immediately
3. **Scan Computer for malware/virus**
4. **Notify**
   a. If hacked account was high profile (email, social media) then notify or post that you've been hacked.
5. **De-Authorize third party apps**
   a. Facebook & Google allow many apps access to your account. Go through and de-authorize them!
      i. https://www.facebook.com/settings?tab=applications
      ii. https://myaccount.google.com/permissions

In the future...

We might not have to rely on passwords as much.

On March 5th, 2019, the W3C approved **WebAuthn as a standard across the internet.** Dropbox and Microsoft are already adopting this standard.

WebAuthn can use a USB key, proxy key, or biometrics to log you into websites.

I guarantee that even after every website uses WebAuthn, some yahoo out there will still use **password1234** as their password!

Thanks for watching!

Questions?
Contact our excellent support team.

805-541-1003
support@landfx.com
www.landfx.com