Hi everyone,

As mentioned, my name is Kyle Erickson, and I'm a Sr. Solution Architect with ICT at the University of Saskatchewan.

Slide 2

For some background on me, I started working at the University of Saskatchewan in 2009 with the Desktop Support group.

Over the years I've obtained a variety of certifications for Windows, Mac, and Linux, and I have a significant amount of experience both professionally and informally helping end users on a wide variety of platforms.

We'll be talking about a variety of things today, and hopefully some of these suggestions will be helpful for you. While the discussion today is all related to keeping you and your devices safe, we'll have a few points where we'll stop to check for questions rather than keep them all to the end. And with that, let's get started.

Slide 3

So what devices am I referring to? For the purposes of this presentation, I'm focusing on:

- Traditional computing devices such as desktops and laptops that run Windows, macOS, or a Linux distribution such as Ubuntu or Fedora.
- Modern devices include an Android phone or tablet, or an iPhone or iPad. Google Chromebooks fit into this category a bit as well as those devices are focused on web browsing and generally easy to maintain compared to a more traditional computing platform like Windows.
- Smart TV's and/or appliances
- Smart home devices such as connected switches, light bulbs, or voice assistants.
- And lastly personal network equipment such as a wireless router or access point.

Slide 4

One of the best things you can do to keep your device safe is to keep it up to date. It's also generally one of the easier things to do.

Most devices are configured to automatically install updates or at least notify you that an update is available. While these updates can sometimes wait a few days if you're busy, it really is important to install updates as soon as possible, particularly for computers, phones, tablets, and even TV's.

Switching back to the previous slide for a moment:

Slide 5

Traditional and modern devices generally hold most of our data, and are also the devices we are using all the time. If your phone was unusable for a day or two it could have a pretty big impact on you.

Windows devices are generally the largest target due to the number of devices out there, but none of the platforms are immune. In May of last year Samsung released an update for most of their smart phones that fixed an issue where a malicious text message could install whatever it wanted on your

phone including ransomware. Just yesterday Apple released updates for iPhone and iPad that could potentially do the same through a malicious website. A factory reset could restore a device to proper working order, but if you lost all your photos, notes, or message history you may not be too happy about it.

Smart TV's are a lower risk, but may be harder to fix when something goes wrong. There was a case in 2016 where someone was browsing the internet on their LG TV that happened to run Android (the same platform as many smart phones). The device became infected with ransomware which likely targeted a vulnerability that was already fixed on newer versions of Android. Unfortunately, the option to factory reset the device wasn't actually available to the end user putting them in a bit of a bind. The ransomware demanded $500 to unlock the device, but LG wasn't much better demanding just shy of $400 to fix it themselves. At that point it was sadly more economical to replace the TV.

Smart switches, bulbs, and such are generally updated through an application on your phone or tablet (which is also generally how they are controlled). Typically these devices are only updated once or twice a year as the function they perform is generally simple leading to less need for regular updates.

I only want to briefly mention personal network equipment as it's probably less common in recent years vs. just using the equipment provided by your internet service provider such as Shaw or SaskTel. A router is a gateway into your home, so for most people it's better to use the providers equipment as they will maintain it. If you have poor Wi-Fi coverage and need something else, check with your provider as most of them now offer additional equipment to extend your wi-fi. Every device on your network connects to the internet through your router, making it an easy point to pivot to and infect other devices on your network so it is important that it is secure.

I think one final thought here is what to do when your equipment isn't supported anymore:

- For computers or phones that you use regularly, you are probably best to consider replacing them.
- For Smart TV's, stick to the pre-installed applications and don't browse the web on them.
- Smart home devices are thus far reasonably low risk and safe, so even after updates end unless an incident occurs, or you encounter compatibility issues I'd probably continue to use it.
- For personal network equipment, consider using the equipment your internet service provider offers instead.

Slide 6

Questions?

Slide 7

The next suggestion that is starting to become easier to do is called DNS filtering. I'll go into the specifics in a moment (including why the word all has a start beside it), but in short it helps to protect all the devices on your network without having to install anything. This is extremely beneficial as it can help to protect devices such as a TV that otherwise are more difficult to protect. The filtering services can also go beyond malicious websites and can also filter adult content to make the internet a bit more family friendly.

Slide 8

So how does it work? DNS is like a phone book for the internet. When you try to go to a website, your device will ask a DNS server what the address is. A DNS filtering service will check the website to see if it's on a block list first, and if it is will return a bogus address instead. At that point you may see an error that the address couldn't be found, or in some cases see nothing at all. The filtering services are usually run by or partnered with large internet companies in positions that allow them to see suspicious traffic in real time and investigate.

So this sounds great, how do you set it up?

Slide 9

There are a few services available, but for most home users I'd recommend CIRA Canadian Shield. CIRA is a non-profit that manages the .ca domain, and they provide a free DNS filtering service to Canadians (including family filters). Shaw also provides a protected browsing service on at least some of their plans. If you travel outside of Canada (or at least if you intend to when things return to some sense of normal), CloudFlare and Quad 9 are other options as well that are available worldwide. Their websites are listed on the slide and they contain instructions on how to configure your devices.

When you configure your router to use these services, all your devices will pick up the DNS filtering service and be protected. So where does the star come from when I mentioned **ALL** devices? It is possible some of your devices will bypass your settings and use a non-filtering DNS service. I'm not really sure of the rationale behind this, but thus far I've seen this behaviour with some of Google's devices like the Chromecast, or Amazon's Fire TV. Despite that, these services help to protect most if not all devices on your network. If you can, it is worth setting up.

Slide 10

Questions about DNS filtering?

Slide 11

Adding on to what we talked about with DNS filtering is ad-blocking. This is generally only possible on computers, phones, or tablets but that's also where it's most necessary. So why do it?

Ad servers are regularly targeted and compromised just like any other server or service. When compromised, malicious ads can be shown across thousands of websites including those you'd normally consider trustworthy.

Ad blockers are typically extensions that you install in a web browser such as Firefox or Chrome. These extensions will look at the content of the page and prevents the advertisements from loading, and it looks like of like this:

Slide 12

This is a traditional website that has 4 ads somewhat overlapping (partly because I made my browser window smaller to capture a smaller screenshot). There is an ad at the top and three along the bottom (two overlapping even).

With an adblocker on:

Slide 13

The content is shifted up and the ads disappear. Not only is the website more enjoyable to view, but you're also far less likely to see something like this:

Slide 14

Generally a malicious ad will take over the browser window, sometimes the whole screen. Most times they require some level of interaction but some won't.

Slide 15

What about sites that rely on ads for revenue that you visit often? If they prompt you to add them to an allow list, consider it. Blocking by default and allowing ads on some websites is better than allowing ads everywhere.

As far as recommendations go, in Firefox and Chrome uBlock Origin is an extremely well regarded and community maintained ad blocking extension. If you use Safari, AdBlock Plus or AdGuard are both good options.

Slide 16

Any questions about ad-blocking?

Slide 17

Next up is password managers. It's not uncommon to use 10 or more services across the internet and most people are guilty of re-using passwords across more than one. Internet companies and services are breached almost daily, and unfortunately a lot of companies do not do a great job protecting your data. Usernames and passwords are dumped onto the internet (or sometimes sold), and then people will use automated tools to check those usernames and passwords on higher value targets like your email account, bank website, or even social media. Password managers help to limit the damage when a service is compromised (so that the password is unique to that service), and they can also help you avoid a look-alike or phishing website that is trying to trick you into entering your credentials. They do this with an autofill service that will check the domain name is the expected domain before filling in the credentials for you. If your password manager isn't filling in the username and password, it will hopefully raise a red flag that you need to take a closer look at the page before proceeding.

Slide 18

A great example is on this slide. Which link looks the most suspicious to you? The poll is already complete but I'll spoil the results slightly for you and reveal that that site with 51.8% of the vote is actually a legitimate website that's basically Google in China. The company was probably playing off the fact that many people outside of China might not know that, but also that the website begins with http instead of https (which indicates a secure connection to the remote server).

The malicious site is actually the third result that "looks" like google.com but the letter "L" is actually a letter "I". Fonts in the browser can sometimes make slight changes like this passable at a quick glance, and there are other tricks related to how we handle other languages in the browser that can make it even worse. But to a password manager, the difference is immediate and obvious.

Slide 19

So what should you use? Most web browsers do include a password manager which is fine if you only have one device or stick with one "ecosystem", such as Apple or Google. If you use multiple platforms using a third party service is likely better. There are free options from companies like LastPass or BitWarden that are accessible in multiple web browsers and across multiple platforms. These services also generally hook in seamlessly on your phone or tablet to even fill passwords in applications for you. They also offer premium services at a cost. Another great option is 1Password which is a Canadian company based in Ontario. The cost is about $4 a month for an individual plan. If you go for 1Password, make sure you go to 1Password.ca, not 1Password.com to ensure your subscription is in Canadian dollars instead of US.

When you use a password manager, you will generally set a strong password or pass "phrase". A phrase could be a sentence like "I was married on July 7th, 2007 in Saskatoon." (and include the punctuation). The only passwords I would skip putting in the password manager and have a separate password for is your primary account, and your online banking which hopefully reduces the number of passwords you have to 3-5 which is more manageable. Your email account is usually what is used to reset the password on another service so it's important to have a strong and unique password for it. And your online banking needs to have the same level of protection as well.

Slide 20

Questions about password managers?

Slide 21

One of the last things I want to talk about is something called multi-factor authentication (or sometimes just two step verification). Multi-factor authentication is when you're combining something you know like a password, with something you have like your phone. The most common is where you will receive a text message after logging in asking for a random one time password (usually a 6 digit code). You know your password, and entering the code can make a service be reasonably confident it is you attempting to log in.

Where multi-factor authentication comes in is for the scenarios where your password is compromised. That could be because of malicious activity on a device, or because you accidentally entered your credentials into a phishing website. Even in those scenarios, without the "something you have" they can't get into your account and it gives you an opportunity to reset your password before any damage is done. It can also alert you to a potential compromise if you start seeing messages pop up on your phone with the code to finish logging in when you aren't expecting it. If you are using a service that offers it, consider setting it up. It does add some complexity, but generally once you're logged in on a device you aren't prompted very often (or even again in some cases).

Side 22

Any questions about multi-factor authentication?

Slide 23

Wrapping things up is antivirus and some other general guidance

Windows and macOS already include built-in protections that are generally sufficient for most users, particularly when combined with DNS filtering and ad-blocking. You can look at third party services such as Sophos Home or MalwareBytes but these services typically try to sell you on value added services beyond antivirus. They may be worth it to you, but I personally stick with the built-in protections combined with DNS filtering and ad-blocking.

Apple and Google both monitor their respective App Stores for iPhone and Android respectively. The best advice for those platforms is to only install applications if you need to. Check the reviews on an application before installing, and check what permissions it is asking for. And of course, keep your devices up to date.

Lastly, be skeptical of pop ups, alerts, text messages, emails, and phone calls. Grammar or spelling mistakes are good indicators something is fake. Demands or offers of money (or gift cards) always require extra scrutiny. Ask yourself if you were expecting a notification/email/call about something particularly when it involves legitimate services such as an Interac e-transfer or tracking for a shipment. And the still useful advise to not click on something if you aren't sure. Go to the website manually, or contact the company if you aren't sure if something is legitimate.

Slide 25

Questions?