AwesomeSafetyBits

Cybersecurity Month

Hello there to our awesome customers! October is National Cybersecurity Month, so we wanted to kick off our newsletter series by taking some time to talk about this hot topic! Cybersecurity is a big buzz word, but actually it all boils down to *Heightened Awareness*. Being aware of the information you are putting out into cyberland and being aware of what is coming back to you. As part of our service to you, we are planning on developing a more robust customer education program to help keep our customers safe and aware of what is going on around you by sharing what we know and what we have seen from a banking and fraud standpoint. The protection of your information is very important to us, so we feel that by educating you on ways to safeguard that information, we will be creating a stronger relationship built on trust and honesty. So here goes- First topic:

What does "Cybersecurity" mean?

Securing your INFORMATION in the CYBER World.

Heightened Awareness. Cybersecurity means understanding the value of your personal data. Keeping your passwords, financial and other personal information safe and protected from ouside intruders. This is **HARD**. It seems like everywhere you turn, you have to provide personal information! Whether it's to log into program/apps or to make purchases on the internet. Figuring out how to protect that information isn't easy, especially if you don't consider yourself **'Tech-Saavy'. Here's a tip.**

If it's EASY FOR YOU- IT'S EASY for the BAD GUYS TOO.

Ask yourself…

- How Strong Are Your Passwords? If they aren't at least 8 characters with an UPPER and lower case and special character (!@#%^$*)- GO CHANGE THEM. **NOW**.
- Do You Use the Same Password for All Websites/Apps? Yeah. Don't do that. Not safe. Easy, ***but not safe***. Keep them different. Or use different variations of the same password for different sites. Try P@$$phrases.
  - o   Rock2Day!   R0cKtwoDay!   !rok2daY   rocktoDAY!
  - o   2DayisGR8!   today!sGrate   tw*daYisGr8   t00dAy!sGreat
- Do You Allow Autofill for Your Passwords? Yep- Not Cool. Sure, it's more convenient- *but not very secure*.
  - o   When the computer asks to remember your password- select NEVER.

Safety starts with **understanding** the VALUE of your *Data.*

AUTO-FILL PASSWORDS

When you save your username and password on a website, it remembers it and will automatically fill it in next time you visit that site. **Super convenient**? *OH YEAH*…**Possibly dangerous**? YOU BETCHA! The internet and third party advertisers are tracking where you go and what you like. They can run scripts in the background to create fake login and password boxes that can capture your credentials and hack your account information; card numbers, addresses, & emails. If you accidentally click a bad link in an email, malware can be downloaded to your computer & could track your autofill login credentials for different sites and simply log in! EEK!!

We recommend using a unique password for every site you visit or make purchases from.

How to turn OFF auto-fill passwords:

Internet Explorer Tools→Internet Options→Content→Autocomplete Settings→ Uncheck the box 'User names and passwords on forms'
Chrome   Menu (3 bars top right) →Settings → Show Advanced Settings→Manage Passwords (in the passwords and forms section)→ Uncheck Enable Autofill & save web passwords
Mozilla Firefox Open Safari Menu (3 bars top right) →Options →Privacy & Security (right toolbar) → Uncheck Ask to save logins and passwords.

Alva State Bank & Trust Company

AwesomeSafetyBits

Understanding Your Digital Footprint   visit https//:www.internetsociety/tutorials.org

A digital footprint is the trail of data you create while using the Internet. It includes the websites you visit, emails you send, and information you submit to online services, like photos, posts, email addresses, passwords, and personal information. Every day, whether we want to or not, most of us contribute to a growing portrait of who we are online; a portrait that is probably more public than most of us assume. So no matter what you do online it is important that you know what kind of trail you are leaving and what the possible side effects can be. As you surf the web, the internet can track your trends and interests and in many cases will sell that information to marketing companies so they can solicit ads that match your interests, hoping you will click and buy their product. When you visit various websites, they can record your IP address that is specific to your computer. That IP address can tell the internet site your geographic location, which web browser you use, what operating system your computer is on and what the last website you visited was. Another tracking system the internet uses is called 'Cookies'. These make the internet more usable and convenient for shoppers by tracking an individual user and adding a layer of security when making purchases. It even helps remember your passwords- which can allow a hacker easy access to your personal accounts. An increased volume of internet surfing can collect an overload of cookies and even make your computer run slower and not function properly.

If you visit the website listed above, there are short tutorials to further explain what it means to leave a digital footprint.

Keeping Your Personal Information Secure Online

Safely Dispose of Personal Information

Encrypt your data.

Read Privacy Agreements & Policies

Don't Overshare on Social Media

Use Security Software

Don't Share your Social Security Number

STAY SMART ONLINE

Be Alert to Impersonators

Lock your device

Keep Passwords Private

Use Anti-virus Software

Be Wise about Wifi

Use Security Software