

ଆଜି ହିଁ ଗ୍ରହଣ କରନ୍ତୁ ନଅଟି ଜରୁରୀ ସାଇବର ସୁରକ୍ଷା ଅଭ୍ୟାସ ।



1. ଆପଣ କ୍ଲିକ୍ କରିବା ପୂର୍ବରୁ ବିରାମ ଦିଅନ୍ତୁ!

ଲିଙ୍କ୍ କ୍ଲିକ୍ କରିବା କିମ୍ବା ସଂଲଗ୍ନକ ଖୋଲିବା ପୂର୍ବରୁ ଦୁଇଥର ଚିନ୍ତା କରନ୍ତୁ, ଯଦିଓ ତୁମେ ଜାଣିଥିବା ବ୍ୟକ୍ତିଙ୍କଠାରୁ ଆସିଥିବାର ଦେଖାଯାଏ ।

- ଅଜ୍ଞାତ ଲିଙ୍କ୍ରେ କ୍ଲିକ୍ କରିବା ପରିବର୍ତ୍ତେ ସର୍ବଦା ଏକ ଜଣାଶୁଣା, ଆଇନଗତ ଉତ୍ସ (ଯଥା HTTPS) ମାଧ୍ୟମରେ ୱେବସାଇଟକୁ ଯାଆନ୍ତୁ ।
- ଯଦି ଏକ ସଂଲଗ୍ନକ ଅପ୍ରତ୍ୟାଶିତ ମନେହୁଏ, ଏକ ବିଶ୍ୱସ୍ତ ପଦ୍ଧତି ମାଧ୍ୟମରେ ପ୍ରେରକଙ୍କ ସହିତ ନିଶ୍ଚିତ କରନ୍ତୁ କିମ୍ବା କ୍ଲିକ୍ ନକରି, ସୁରକ୍ଷିତ ପାର୍ଶ୍ୱରେ ରହିବାକୁ ବାଛନ୍ତୁ ।



2. ବ୍ୟକ୍ତିଗତ ସୂଚନା ପାଇଁ ଅନୁରୋଧ ଯାଞ୍ଚ କରନ୍ତୁ

ସର୍ବଦା ବ୍ୟକ୍ତିଗତ ତଥ୍ୟ ପାଇଁ ଅନୁରୋଧ ନିଶ୍ଚିତ କରନ୍ତୁ - ଏହା ଆପଣଙ୍କର କିମ୍ବା ଅନ୍ୟ କାହାର ।

- ସ୍କାମର ମାନେ ବିଶ୍ୱସ୍ତ ସମ୍ପର୍କକୁ ସହଜରେ ଛଦ୍ମନାମ କରିପାରିବେ ।
- ଅସାଧାରଣ କାର୍ଯ୍ୟକଳାପ ପାଇଁ ନିୟମିତ ଭାବରେ ଆର୍ଥିକ ବିବରଣୀ ଏବଂ କ୍ରେଡିଟ୍ ରିପୋର୍ଟ ସମୀକ୍ଷା କରନ୍ତୁ ।
- ଅନେକ ଫିସିଂ ବାର୍ତ୍ତା ବନାନ ଏବଂ ବ୍ୟାକରଣଗତ ତ୍ରୁଟି ଧାରଣ କରିଥାଏ ।
- ଅନୁରୋଧ ଆଇନଗତ କି ନୁହେଁ ତାହା ବିଚାର କରନ୍ତୁ । ସେହି ବ୍ୟକ୍ତି କିମ୍ବା ସଂସ୍ଥାର ସେହି ସୂଚନା ଆବଶ୍ୟକତା ଅଛି କି ?



3. ଆପଣଙ୍କର ପାସୱାର୍ଡଗୁଡ଼ିକୁ ନିୟନ୍ତ୍ରଣ କରନ୍ତୁ ।

ଶକ୍ତିଶାଳୀ, ଜଟିଳ ପାସୱାର୍ଡ ସୃଷ୍ଟି କରିବା ଏବଂ ବୁଦ୍ଧିମାନ ଭାବରେ ପରିଚାଳନା କରିବା ଆପଣଙ୍କ ଆକାଉଣ୍ଟକୁ ସୁରକ୍ଷିତ ରଖିବା ପାଇଁ ଜରୁରୀ

- ବିଭିନ୍ନ ଖାତା ପାଇଁ ଅନନ୍ୟ ପାସୱାର୍ଡ ବ୍ୟବହାର କରନ୍ତୁ ।
- କାର୍ଯ୍ୟ ଏବଂ ବ୍ୟକ୍ତିଗତ ପାସୱାର୍ଡଗୁଡ଼ିକୁ ଅଲଗା ରଖନ୍ତୁ ।
- ପାସୱାର୍ଡ କେବେବି ସେୟାର କରନ୍ତୁ ନାହିଁ ।
- ବାରମ୍ବାର ପାସୱାର୍ଡ ପରିବର୍ତ୍ତନ କରନ୍ତୁ ।
- ବ୍ରାଉଜରରେ ପାସୱାର୍ଡ ସେଭ୍ କରିବାକୁ ବାଦ୍ ଦିଅନ୍ତୁ ।
- ଅତିରିକ୍ତ ସୁରକ୍ଷା ପାଇଁ ମଲ୍ଟି ଫ୍ୟାକ୍ଟର ପ୍ରାମାଣିକିକରଣ (MFA)କୁ ସକ୍ରିୟ କରନ୍ତୁ ।



4. ଆପଣଙ୍କର ଉପକରଣଗୁଡ଼ିକୁ ସୁରକ୍ଷିତ କରନ୍ତୁ ।

ଆପଣଙ୍କର କାର୍ଯ୍ୟକ୍ଷେତ୍ରକୁ ଲକ୍ ଅଫ୍ କରନ୍ତୁ ଏବଂ ଦୂରକୁ ଯିବାବେଳେ ଆପଣଙ୍କର ଉପକରଣଗୁଡ଼ିକୁ ସୁରକ୍ଷିତ କରନ୍ତୁ ।

- ସର୍ବଦା ଆପଣଙ୍କର କମ୍ପ୍ୟୁଟର ସ୍କ୍ରିନ୍ ଲକ୍ କରନ୍ତୁ ।
- ଆପଣଙ୍କ ଫୋନ୍ ଏବଂ ପୋର୍ଟେବଲ୍ ଡିଭାଇସ୍ ସାଙ୍ଗରେ ନିଅନ୍ତୁ କିମ୍ବା ସେଗୁଡ଼ିକୁ ସୁରକ୍ଷିତ ଭାବରେ ଗଚ୍ଛିତ କରନ୍ତୁ ।
- ଯେତେବେଳେ ସମ୍ଭବ ଶକ୍ତିଶାଳୀ ପ୍ରାମାଣିକିକରଣ ପଦ୍ଧତି ବ୍ୟବହାର କରନ୍ତୁ ।



5. ଗୁରୁତ୍ୱପୂର୍ଣ୍ଣ ଫାଇଲଗୁଡ଼ିକର ନକଲ ସଂରକ୍ଷଣ କରନ୍ତୁ ।

ନିଶ୍ଚିତ କରନ୍ତୁ ଯେ ଆପଣଙ୍କର ଜଟିଳ ତଥ୍ୟ ନିୟମିତ ବ୍ୟାକଅପ୍ ହୋଇଛି ।

- ମୂଳ ସ୍ଥାନରୁ ଅଲଗା ସ୍ଥାନରେ ବ୍ୟାକଅପ୍ ଗଚ୍ଛିତ କରନ୍ତୁ ।
- ସଂଗଠନ-ଅନୁମୋଦିତ ସଂରକ୍ଷଣ ସମାଧାନ ବ୍ୟବହାର କରନ୍ତୁ ।
- ସେଗୁଡ଼ିକ ସଠିକ୍ ଭାବରେ କାର୍ଯ୍ୟ କରିବା ପାଇଁ ନିୟମିତ ଭାବରେ ବ୍ୟାକଅପ୍ ପରୀକ୍ଷା କରନ୍ତୁ ।



6. ସନ୍ଦେହଜନକ କାର୍ଯ୍ୟକଳାପ ରିପୋର୍ଟ କରନ୍ତୁ ।

ଯଦି କିଛି ସନ୍ଦେହଜନକ ମନେହୁଏ, ତୁମର ପ୍ରବୃତ୍ତି ଉପରେ ବିଶ୍ୱାସ କର - ଏହାକୁ ରିପୋର୍ଟ କର!

- ସନ୍ଦେହଜନକ ସ୍କାମ କିମ୍ବା ସନ୍ଦେହଜନକ କାର୍ଯ୍ୟକଳାପ ପାଇଁ ତୁମର ସୁପରଭାଇଜରଙ୍କୁ ସତର୍କ କର ଏବଂ ତୁମର ସଂସ୍ଥାର ରିପୋର୍ଟିଂ ପ୍ରୋଟୋକଲ୍‌କୁ ଅନୁସରଣ କର ।



7. ନିଜକୁ ଏବଂ ଅନ୍ୟମାନଙ୍କୁ ଶିକ୍ଷା ଦିଅ ।

ଅତ୍ୟାଧୁନିକ ସାଇବର ସୁରକ୍ଷା ବିପଦ ଏବଂ ଧାରା ବିଷୟରେ ଅବଗତ ରୁହନ୍ତୁ ।

- ପ୍ରଶିକ୍ଷଣ ଅଧିବେଶନରେ ଯୋଗ ଦିଅନ୍ତୁ ଏବଂ ଯେତେବେଳେ ଆପଣ ଏକ ସୁଯୋଗ ପାଇବେ ସହକର୍ମୀମାନଙ୍କ ସହିତ ଜ୍ଞାନ ବାଣ୍ଟନ୍ତୁ ।
- ଏକ ସୁଚିତ୍ରିତ ଦଳ ହେଉଛି ସାଇବର ବିପଦରୁ ରକ୍ଷା କରିବାର ପ୍ରଥମ ଧାଡ଼ି ।



8. ସୁରକ୍ଷିତ ନେଟୱାର୍କ ବ୍ୟବହାର କରନ୍ତୁ ।

ବିଶେଷତଃ ସମ୍ବେଦନଶୀଳ ସୂଚନାକୁ ପ୍ରବେଶ କରିବା ସମୟରେ, ସର୍ବଦା ସୁରକ୍ଷିତ ନେଟୱାର୍କ ସହିତ ସଂଯୋଗ କରନ୍ତୁ ।

- ଆର୍ଥିକ କାରବାର କିମ୍ବା ସମ୍ବେଦନଶୀଳ କାର୍ଯ୍ୟ ପାଇଁ ସର୍ବସାଧାରଣ ୱାଇ-ଫାଇରୁ ଦୂରେଇ ରୁହନ୍ତୁ ।
- ଅତିରିକ୍ତ ସୁରକ୍ଷା ପାଇଁ ଆବଶ୍ୟକ ସମୟରେ ଭର୍ଚୁଆଲ୍ ପ୍ରାଇଭେଟ ନେଟୱାର୍କ (VPN) ବ୍ୟବହାର କରନ୍ତୁ ।



9. ସୋସିଆଲ ମିଡିଆ ସହିତ ସତର୍କ ରୁହନ୍ତୁ ।

ଆପଣ ଅକ୍ଲିଭରେ ସେୟାର କରୁଥିବା ବ୍ୟକ୍ତିଗତ ସୂଚନା ପରିମାଣକୁ ସୀମିତ କରନ୍ତୁ । ତେଣୁ ଆପଣ ଆପଣଙ୍କର ଗୋପନୀୟତା ରକ୍ଷା କରିପାରିବେ, ଆପଣଙ୍କର ସୁରକ୍ଷାକୁ ବଢାଇ ପାରିବେ ଏବଂ ଏକ ଅଧିକ ସକରାତ୍ମକ ଅନୁଭବ ଅଭିଜ୍ଞତା ସୃଷ୍ଟି କରିପାରିବେ ।

- ସୋସିଆଲ ମିଡିଆ ପ୍ଲାଟଫର୍ମରେ ଗୋପନୀୟତା ସେଟିଂସମାନଙ୍କୁ ସମୀକ୍ଷା କରନ୍ତୁ ।
- ବନ୍ଧୁ ଅନୁରୋଧ ଏବଂ ଆପଣଙ୍କର ସୂଚନାକୁ କିଏ ପ୍ରବେଶ କରେ ସେଥିପ୍ରତି ଧ୍ୟାନ ଦିଅନ୍ତୁ ; ଏକ ଲକ୍ ହୋଇଥିବା ପ୍ରୋଫାଇଲରୁ ଅନୁରୋଧ ଗ୍ରହଣ କରନ୍ତୁ ନାହିଁ ।
- ସମ୍ଭାବ୍ୟ ବିପଦକୁ କମ୍ କରିବାକୁ ନିୟମିତ ଭାବରେ ଆପଣଙ୍କର ଅନୁଭବ ଉପସ୍ଥିତି ଅତିର୍କ କରନ୍ତୁ ।

ମନେରଖ: ସାଇବର ସିକ୍ୟୁରିଟି ହେଉଛି ସମସ୍ତଙ୍କର ଦାୟିତ୍ବବୋଧ!