

ପରିଶିଷ୍ଟ 7: ଗ୍ରାହକ ସଚେତନତା-ସାଇବର ଧମକ ଏବଂ ଠକେଇ

ଏହା ଦେଖାଯାଇଛି ଯେ ଅନୈତିକ ଡକ୍ସ ଗୁଡ଼ିକ ସୋସିଆଲ ମିଡ଼ିଆ କୌଶଳ, ମୋବାଇଲ ଫୋନ୍ କଲ୍ ଇତ୍ୟାଦି ସହିତ ଅଭିନବ କାର୍ଯ୍ୟ ପଦ୍ଧତି ଉପଯୋଗ କରି ଜନସାଧାରଣଙ୍କୁ ପ୍ରତାରଣା କରୁଛନ୍ତି ଏବଂ ବିଭ୍ରାନ୍ତ କରୁଛନ୍ତି । ଏହାକୁ ଦୃଷ୍ଟିରେ ରଖି ଡିସିବି ବ୍ୟାଙ୍କ ଜନସାଧାରଣଙ୍କୁ ଜାଲିଆତି କରୁଥିବା ବାର୍ତ୍ତା, ବିଭ୍ରାନ୍ତ କଲ୍, ଅଜ୍ଞାତ ଲିଙ୍କ, ମିଥ୍ୟା ବିଜ୍ଞପ୍ତି, ଅନଧିକୃତ କ୍ୟୁଆର୍ କୋଡ୍ ଇତ୍ୟାଦି ବିଷୟରେ ସଚେତନ ହେବାକୁ ଚେତାବନୀ ଦେଇଛି, ବ୍ୟାଙ୍କ ଏବଂ ବିଭ୍ରାନ୍ତ ସେବା ପ୍ରଦାନକାରୀଙ୍କ ଠାରୁ କୌଣସି ବି ପ୍ରକାର ରିହାତି / ଦ୍ୱରାଦ୍ୱିତ ପ୍ରତିକ୍ରିୟା ପାଇବାରେ ସାହାଯ୍ୟ କରିବାର ପ୍ରତିଶ୍ରୁତି ଦେଇଛି ।

ଠକମାନେ ଗୁପ୍ତ ତଥ୍ୟ ପାଇବାକୁ ଚେଷ୍ଟା କରନ୍ତି ଯେପରିକି ଯୁକ୍ତର ଆଇଡି, ଲଗିନ୍ / ଗ୍ରାଞ୍ଜାକଶନ୍ ପାସୱାର୍ଡ, ଡ୍ରାନ୍ ଟାଇମ୍ ପାସୱାର୍ଡ (ଓଟିପି), ଡେବିଟ୍ / କ୍ରେଡିଟ୍ କାର୍ଡ ବିବରଣୀ ଯେପରିକି ପିନ୍, ସିଭିଭି, ମିଆବ ପୂର୍ଣ୍ଣ ତାରିଖ ଏବଂ ଅନ୍ୟାନ୍ୟ ବ୍ୟକ୍ତିଗତ ସୂଚନା ଇତ୍ୟାଦି । ଠକମାନଙ୍କ ଦ୍ୱାରା ବ୍ୟବହାର ହେଉଥିବା ସାଧାରଣ ବିଶେଷ କାର୍ଯ୍ୟପ୍ରଣାଳୀ:

- କେଣ୍ଡାଇସି ଅପଡେଟ୍ କରିବା, ଖାତା/ସିମ୍ କାର୍ଡ ଅନବୁକ୍ କରିବା, ଡେବିଟ୍ ରାଶି ଜମା କରିବା ଆଦି ବାହାନା କରି ଗୋପନୀୟ ବିବରଣୀ ଶେୟର୍ କରିବା ପାଇଁ ଗ୍ରାହକଙ୍କୁ ଲୋଭାଣୁଛନ୍ତି କରିବା ପାଇଁ ବ୍ୟାଙ୍କ / ଅଣ-ବ୍ୟାଙ୍କ ଇ-ଫ୍ରିଣ୍ଡଲି ପ୍ରଦାନକାରୀ / ଟେଲିକମ ସେବା ପ୍ରଦାନକାରୀଙ୍କଠାରୁ ଭିଶି-ଫୋନ୍ କଲ୍ ।
- ଫିଶିଂ - ଧୋକାକାରୀ ଇମେଲ୍ ଏବଂ / କିମ୍ବା ଏସଏମଏସ୍ ଗ୍ରାହକଙ୍କୁ ଏହା ଭାବିବା ପାଇଁ ଡିଜାଇନ୍ ହୋଇଛି ଯେ ଯୋଗାଯୋଗ ସେମାନଙ୍କ ବ୍ୟାଙ୍କ / ଇ-ଫ୍ରିଣ୍ଡଲି ପ୍ରଦାନକାରୀଙ୍କଠାରୁ ଆସିଛି ଏବଂ ଗୁପ୍ତ ବିବରଣୀ ବାହାର କରିବାକୁ ଲିଙ୍କ ସାମିଲ ଅଛି ।
- ରିମୋଟ୍ ଆକ୍ସେସ୍ - ଗ୍ରାହକମାନଙ୍କୁ ସେମାନଙ୍କ ମୋବାଇଲ ଫୋନ୍ / କମ୍ପ୍ୟୁଟରରେ ଏକ ଆପ୍ଲିକେସନ୍ ଡାଉନଲୋଡ୍ କରିବାକୁ ପ୍ରଲୋଭିତ କରି ଯାହା ଗ୍ରାହକଙ୍କ ଡିଭାଇସ୍ରେ ଥିବା ତଥ୍ୟକୁ ବ୍ୟବହାର କରିପାରିବ ।
- ପଇସା ପାଇଁ ‘ଆପଣଙ୍କ ଯୁପିଆଇ ପିନ୍ ପ୍ରବେଶ କରନ୍ତୁ’ ପରି ସନ୍ଦେଶ ସହିତ ନକଲି ଦେୟ ଅନୁରୋଧ ପଠାଇ ‘ସଂଗ୍ରହ ଅନୁରୋଧ’ ସୁବିଧାର ଅପବ୍ୟବହାର ।
- ଫ୍ରେବପେଜ୍ / ସୋସିଆଲ ମିଡ଼ିଆରେ ବ୍ୟାଙ୍କ / ଇ-ଫ୍ରିଣ୍ଡଲି ପ୍ରଦାନକାରୀଙ୍କ ନକଲି କଣ୍ଟାକୁ ନମ୍ବର ଏବଂ ସର୍ଚ୍ଚ ଇଞ୍ଜିନ୍ ଦ୍ୱାରା ପ୍ରଦର୍ଶିତ ଇତ୍ୟାଦି ।

ଡିସିବି ବ୍ୟାଙ୍କ ଯେକୌଣସି ଡିଜିଟାଲ (ଅନଲାଇନ୍ / ମୋବାଇଲ) ବ୍ୟାଙ୍କିଙ୍ଗ୍ / ପେମେଣ୍ଟ କାରବାର କରୁଥିବାବେଳେ ସମସ୍ତ ସତର୍କତା ଅବଲମ୍ବନ କରି ସୁରକ୍ଷିତ ଡିଜିଟାଲ ବ୍ୟାଙ୍କିଙ୍ଗ୍ ଅଭ୍ୟାସ କରିବାକୁ ଜନସାଧାରଣଙ୍କୁ ଅନୁରୋଧ କରୁଛି । ଏଗୁଡ଼ିକ ଆର୍ଥିକ ଏବଂ / କିମ୍ବା ଅନ୍ୟାନ୍ୟ କ୍ଷତି ରୋକିବାରେ ସାହାଯ୍ୟ କରିବ ।

ସୁରକ୍ଷିତ ଡିଜିଟାଲ ବ୍ୟାଙ୍କିଙ୍ଗ୍ ଅଭ୍ୟାସ

- ଆପଣଙ୍କର ଆକାଉଣ୍ଟ ବିବରଣୀ ଯେପରିକି ଆକାଉଣ୍ଟ ନମ୍ବର, ଲଗିନ୍ ଆଇଡି, ପାସୱାର୍ଡ, ପିନ୍, ଯୁପିଆଇ-ପିନ୍, ଓଟିପି, ଏଟିଏମ୍/ ଡେବିଟ୍ କାର୍ଡ / କ୍ରେଡିଟ୍ କାର୍ଡ ବିବରଣୀ କାହା ସହିତ ଶେୟର୍ କରନ୍ତୁ ନାହିଁ, ବ୍ୟାଙ୍କ ଅଧିକାରୀଙ୍କ ସହିତ ମଧ୍ୟ ନୁହେଁ, ଯଦିଓ ସେମାନେ ପ୍ରକୃତ ପରି ଲାଗିଥାନ୍ତି ।
- କେଣ୍ଡାଇସିର ଅପଡେଟ୍ ନହେବା ବାହାନାରେ ଆପଣଙ୍କ ଆକାଉଣ୍ଟକୁ ଅବରୋଧ କରିବାର ଧମକ ଦେଉଥିବା ଯେକୌଣସି ଫୋନ୍ କଲ୍ / ଇମେଲ୍ ଏବଂ ଏହାକୁ ଅପଡେଟ୍ କରିବା ପାଇଁ ଲିଙ୍କ ଉପରେ କ୍ଲିକ୍ କରିବାର ପରାମର୍ଶ ଦେବା ଠକମାନଙ୍କର ଏକ ସାଧାରଣ କାର୍ଯ୍ୟପ୍ରଣାଳୀ ଅଟେ । ସର୍ବଦା ଆପଣଙ୍କର ବ୍ୟାଙ୍କ / ଏନ୍-ଏଫ୍-ସି / ଇ-ଫ୍ରିଣ୍ଡଲି ପ୍ରଦାନକାରୀଙ୍କ ଅଫିସିଆଲ ୱେବସାଇଟ୍କୁ ବ୍ୟବହାର କରନ୍ତୁ କିମ୍ବା ଶାଖା ସହିତ ଯୋଗାଯୋଗ କରନ୍ତୁ ।
- ଆପଣଙ୍କ ଫୋନ୍ କିମ୍ବା ଡିଭାଇସ୍ରେ କୌଣସି ଅଜ୍ଞାତ ଆପ୍ ଡାଉନଲୋଡ୍ କରନ୍ତୁ ନାହିଁ । ଏହି ଆପ୍ ଗୁପ୍ତ ଭାବରେ ଆପଣଙ୍କର ଗୋପନୀୟ ତଥ୍ୟକୁ ବ୍ୟବହାର କରିପାରେ ।
- ମନି ରସିଦ୍ ସହିତ ଜଡିତ କାରବାର ଗୁଡ଼ିକ ବାରକୋଡ୍ କିମ୍ବା କ୍ୟୁଆର୍ କୋଡ୍ ସ୍କାନ କରିବା କିମ୍ବା ଏମପିନ୍ ପ୍ରବେଶ କରିବା ଆବଶ୍ୟକ କରେ ନାହିଁ । ତେଣୁ, ଯଦି ଏହା କରିବାକୁ କୁହାଯାଏ ତେବେ ସତର୍କତା ଅବଲମ୍ବନ କରନ୍ତୁ ।
- ଯୋଗାଯୋଗ ବିବରଣୀ ପାଇଁ ସର୍ବଦା ବ୍ୟାଙ୍କ / ଏନ୍-ଏଫ୍-ସି / ଇ-ଫ୍ରିଣ୍ଡଲି ପ୍ରଦାନକାରୀଙ୍କ ଅଫିସିଆଲ ୱେବସାଇଟ୍କୁ ବ୍ୟବହାର କରନ୍ତୁ । ଇଣ୍ଟରନେଟ୍ ସର୍ଚ୍ଚ ଇଞ୍ଜିନ୍ରେ ଯୋଗାଯୋଗ ନମ୍ବର ଠକମାନଙ୍କ ଦ୍ୱାରା ହୋଇପାରେ ।
- ବନାନ ତୁଟି ପାଇଁ ଇମେଲ୍ ଏବଂ ଏସଏମଏସ୍ରେ ପ୍ରାପ୍ତ ଯୁଆରଏଲ୍ ଏବଂ ଡୋମେନ୍ ନାମ ଯାଞ୍ଚ କରନ୍ତୁ । ଅନଲାଇନ୍ ବ୍ୟାଙ୍କିଙ୍ଗ୍ ପାଇଁ କେବଳ ଯାଞ୍ଚ ହୋଇଥିବା, ସୁରକ୍ଷିତ ଏବଂ ବିଶ୍ୱସ୍ତ ୱେବସାଇଟ୍ ଏବଂ ଆପ୍ ବ୍ୟବହାର କରନ୍ତୁ, ଯାହାର ୱେବସାଇଟ୍ “https” ରୁ ଆରମ୍ଭ ହୋଇଥାଏ । ଏକ ସନ୍ଦିଗ୍ଧ ଯୁଆରଏଲ୍ କିମ୍ବା ୱେବସାଇଟ୍ ତୁରନ୍ତ ସ୍ଥାନୀୟ ପୋଲିସ୍ / ସାଇବର ଅପରାଧ ଶାଖାକୁ ସୂଚିତ କରାଯିବା ଉଚିତ ।

- ଆପଣଙ୍କ ଦ୍ୱାରା ଆରମ୍ଭ ହୋଇଥିବା କାରବାର ପାଇଁ ଯଦି ଆପଣ ଆପଣଙ୍କ ଆକାଉଣ୍ଟକୁ ଡେବିଟ୍ କରିବା ପାଇଁ ଏକ ଡିବିଡିଏ ପ୍ରକ୍ରିୟା କରନ୍ତେ, ତେବେ ତୁରନ୍ତ ଆପଣଙ୍କ ବ୍ୟାଙ୍କ / ଇ-ଡ୍ରାଲେଟ୍ ପ୍ରଦାନକାରୀଙ୍କୁ ଜଣାନ୍ତୁ । ଯଦି କାରବାର ହୋଇନଥିଲେ ବି ଆପଣ ଏକ ଡେବିଟ୍ ଏସଏମଏସ୍ ଗ୍ରହଣ କରନ୍ତି, ତେବେ ତୁରନ୍ତ ଆପଣଙ୍କର ବ୍ୟାଙ୍କ / ଇ-ଡ୍ରାଲେଟ୍ ପ୍ରଦାନକାରୀଙ୍କୁ ଜଣାନ୍ତୁ ଏବଂ ଯୁପିଆଇ ସମେତ ସମସ୍ତ ପଦ୍ଧତିର ଡେବିଟ୍‌କୁ ଅବରୋଧ କରନ୍ତୁ । ଯଦି ଆପଣ ଆପଣଙ୍କ ଆକାଉଣ୍ଟରେ କୌଣସି ଠକାମି କାର୍ଯ୍ୟକଳାପକୁ ସନ୍ଦେହ କରୁଛନ୍ତି, ଇଣ୍ଟରନେଟ୍ / ମୋବାଇଲ୍ ବ୍ୟାଙ୍କିଙ୍ଗ୍ ପାଇଁ ସକ୍ଷମ ହିତାଧିକାରୀ ତାଲିକାରେ ଯୋଗ ପାଇଁ ଯାଚ୍ଛ କରନ୍ତୁ ।
- ଆପଣଙ୍କ ବ୍ୟାଙ୍କ / ଇ-ଡ୍ରାଲେଟ୍ ଆକାଉଣ୍ଟ ସହିତ ଲିଙ୍କ୍ ହୋଇଥିବା ଆପଣଙ୍କର ଇମେଲ୍ ପାସପୋର୍ଟ ଶେୟାର କରନ୍ତୁ ନାହିଁ । ଇ-କମର୍ସ / ସୋସିଆଲ ମିଡିଆ ସାଇଟ୍ ଏବଂ ଆପଣଙ୍କର ବ୍ୟାଙ୍କ ଆକାଉଣ୍ଟ ଏବଂ ଆପଣଙ୍କ ବ୍ୟାଙ୍କ ଆକାଉଣ୍ଟ ପାଇଁ ଲିଙ୍କ୍‌ଡ ଇମେଲ୍ ପାଇଁ ସାଧାରଣ ପାସପୋର୍ଟ ଦିଅନ୍ତୁ ନାହିଁ । ସାର୍ବଜନିକ, ଖୋଲା କିମ୍ବା ମାଗଣା ଡ୍ରା-ଫାଲ କିମ୍ବା ଇଣ୍ଟରନେଟ୍ ନେଟୱାର୍କ ମାଧ୍ୟମରେ ବ୍ୟାଙ୍କିଂ ଠାରୁ ଦୂରରେ ରୁହନ୍ତୁ ।
- ଆପଣଙ୍କ ଯୁକ୍ତ ଆଇଡି ରୂପେ ଇମେଲ୍ ସହିତ କୌଣସି ଡ୍ରେବସାଇଟ୍ / ଆପ୍ଲିକେସନ୍‌ରେ ପଞ୍ଜୀକୃତ କରିବା ବେଳେ ଆପଣଙ୍କର ଇମେଲ୍ ପାସପୋର୍ଟକୁ ପାସପୋର୍ଟ ଶବ୍ଦ ଭାବରେ ସେଟ୍ କରନ୍ତୁ ନାହିଁ । ଆପଣଙ୍କ ଇମେଲ୍‌କୁ ଆକସେସ୍ କରିବା ପାଇଁ ବ୍ୟବହୃତ ପାସପୋର୍ଟ, ବିଶେଷତ ଯଦି ଆପଣଙ୍କର ବ୍ୟାଙ୍କ ଆକାଉଣ୍ଟ ସହିତ ଲିଙ୍କ୍ ହୁଏ, ଅନନ୍ୟ ହେବା ଉଚିତ ଏବଂ କେବଳ ଇମେଲ୍ ପ୍ରବେଶ ପାଇଁ ବ୍ୟବହାର କରାଯିବା ଉଚିତ ଏବଂ ଅନ୍ୟ କୌଣସି ଡ୍ରେବସାଇଟ୍ କିମ୍ବା ଆପ୍ଲିକେସନ୍ ବ୍ୟବହାର କରିବା ପାଇଁ ବ୍ୟବହୃତ ହେବା ଅନୁଚିତ ।
- ବିଦେଶ ଅର୍ଥ ପ୍ରେରଣ, କମିଶନ୍‌ର ରସିଦ୍ କିମ୍ବା ଲଗେରା ଜିଡିବା ପାଇଁ ଆର୍ବିଆଇ ସହିତ ଆପଣଙ୍କ ଡରଫରୁ ଟଙ୍କା ଜମା କରିବାକୁ ପରାମର୍ଶ ଦେଇ ଭ୍ରମିତ ହୁଅନ୍ତୁ ନାହିଁ ।
- ଆପଣଙ୍କର ଆର୍ଥିକ ସେବା ପ୍ରଦାନକାରୀଙ୍କ ଚେତାବନୀ ପାଇଁ ନିୟମିତ ଭାବରେ ଆପଣଙ୍କର ଇମେଲ୍ ଏବଂ ଫୋନ୍ ବାର୍ତ୍ତା ଯାଚ୍ଛ କରନ୍ତୁ । ଅଧିକ କ୍ଷତି ନହେବା ପାଇଁ କାର୍ଡ, ଆକାଉଣ୍ଟ, ଡ୍ରାଲେଟ୍‌କୁ ଅବରୋଧ କରିବା ପାଇଁ ଆପଣଙ୍କ ଆକାଉଣ୍ଟରେ ଥିବା ଯେକୌଣସି ଅନଧିକୃତ କାରବାର ବିଷୟରେ ତୁରନ୍ତ ଆପଣଙ୍କ ବ୍ୟାଙ୍କ / ଏନ୍‌ଏସ‌ଏସ୍ / ସେବା ପ୍ରଦାନକାରୀଙ୍କୁ ରିପୋର୍ଟ କରନ୍ତୁ ।
- ଆପଣଙ୍କ ଏଟିଏମ୍, ଡେବିଟ୍ ଏବଂ କ୍ରେଡିଟ୍ କାର୍ଡକୁ ସୁରକ୍ଷିତ କରନ୍ତୁ ଏବଂ କାରବାର ପାଇଁ ଦୈନିକ ସୀମା ସ୍ଥିର କରନ୍ତୁ । ଆପଣ ମଧ୍ୟ ସୀମା ସ୍ଥିର କରିପାରିବେ ଏବଂ ଘରୋଇ / ଆନ୍ତର୍ଜାତୀୟ ବ୍ୟବହାର ପାଇଁ ସକ୍ରିୟ / ନିଷ୍କ୍ରିୟ କରିପାରିବେ । ଏହା ଠକାମି ଜନିତ କ୍ଷତିକୁ ସୀମିତ କରିପାରେ ।