6.Preventive measures to be taken in Cyber Space

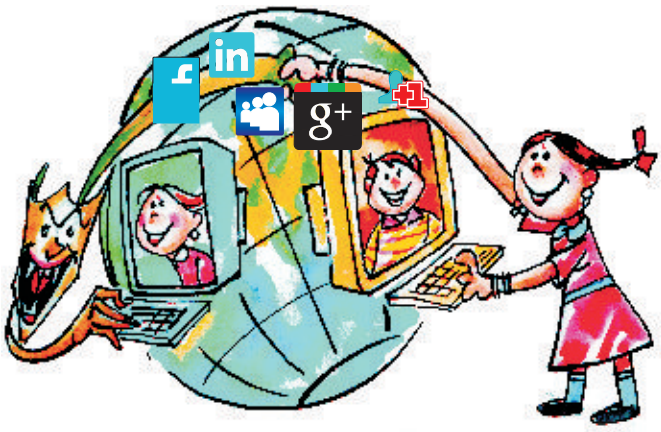
- **Don't give your personal details of where abouts** : Don't post specific personal information online, such as travel dates, location and time of the movie you plan to watch, evening classes that you take etc.,
- **Keep contact information private :** Beware of strangers.
- **Friends :** Better avoid strangers as friends when requests are received.
- Don't share your personal information irrespective of genders as they may post abusive/indecent messages when the relations are strained with them.

Be aware of following risks

Spam

As we all know that spam is usually unwanted e-mail advertising about a product sent to list of e-mails or group of e-mail addresses. Similarly spammers are sending the unwanted mails or messages to the billions of users of social networking sites which are free; and is easily accessable by spammers to gather the personal information of the unsuspecting users.

Always use updated spam-blocking software.



Scams

Online scammers generally send an e-mail or message with a link to the user which ask for the profile information and tells the user that it would add new followers.These links sent to the user would be similar to applications, games etc. So whenever the user post his details in the link then the details will be received by scammers and information would be misused.

Malicious applications

Malicious application might come through different application while using or installing software. Similarly, if we click on links in the social networking any application starts the installation process or link to view the video, etc. In order to fulfil its intended operation the application requests for some elevated privileges from the user like access to my basic information , update on my wall, post on my wall, etc .

Clickjacking

Generally, clickjacking is a malicious technique of tricking Web users into revealing confidential information or taking control of their computer while clicking on seemingly innocuous Web pages. Vulnerability across a variety of browsers and platforms, a clickjacking takes the form of embedded code or script that can run without the user's knowledge. The same is followed in the social networking domain. The objective behind such an attack is that users can be tricked into clicking in the links, icons, buttons etc, which could trigger running of processes at the background without the knowledge of the user.

Phishing

As we all know the phishing attack is creation of fake site just similar to original site. Similarly these days even social networking phishing has come in different flavours just like phishing attacks on banks and popular trading websites. Social networking phishing has come up with fake mails and messages like offering some specialized themes, updating the profile, updating the security application/features etc. In order to see the updates the user needs to follow a link and log in, through which the credentials are taken by the attacker. The linked page is a fake copy of the original login page, focused on stealing user account credentials.

Be aware of phishing e-mail scams

Guidelines:

- Don't give or post any personal information like your name, address of the school / home, phone numbers, age, sex, credit card details.
- The information which was posted by you in online can be seen by everyone who is online because internet is the world's biggest information exchange tool. Many people who are having access to the site which you are using can access your profile and get all the information what you have posted. The persons who is having access to your profile may include good persons like your friends, parents, teachers and bad persons like strangers.
- Be aware that the information you give in the sites could also put you at risk of victimization
- Never give out your password to anyone other than your parent or guardian.
- Change your password frequently, and avoid clicking links that purport to send you back to the social network site. Instead, type the site's address directly into your browser (or follow a bookmark you've previously saved) to get back to your account.
- When you are choosing a Social Networking site, privacy issues should be considered.
- While accepting the friends on Social Networking sites, be selective. Only add people as friends to your site if you know them in real life.
- Never meet in person with anyone whom you met on Social Networking site because some of the people may not be who they say they are.
- Take your parents permission if you want to meet the person whom you met in the networking site.
- Most of the Social Networking web sites enabling users to set privacy controls for who has the ability to view the information.So try to use such facilities.
- Do not post anything which harm to your family credibility.
- Never post photographs, videos and any other sensitive information to unknown persons in Social network sites.
- If you think that your social networking account details have been compromised or stolen, report your suspicions to the networking site support team immediately.
- Never respond to harassing or rude comments which are posted on your profile.
- Delete any unwanted messages or friends who continuously leave inappropriate comments and immediately report those comments to the networking site.
- Do not post your friends information in networking sites, which may possibly put them at risk. Protect your friends by not posting the group photos, school names, locations, ages, sex...etc.
- Avoid posting the plans and activities which you are going to do in networking sites.
- Check the privacy settings of the Social Networking sites and set the settings in such a way that the people can only be added as your friend if you approve them also set the settings in such a way that the people can only view your profile if you have approved them as a friend.

6. సైబర్ స్పేస్ లో తీసుకోవలసిన నివారణ చర్యలు

- మీ వ్యక్తిగత వివరములను ఇవ్వకండి : ప్రయాణాల తేదీలను, మీరు చూచుటకు వెళుతున్న సినిమా సమయము మరియు స్థల వివరములు , సాయంత్ర వేళ వెళ్ళు క్లాసుల వివరములు మొదలగు మీ వ్యక్తిగత వివరములను ఆన్‌లైన్ లో ఇవ్వకూడదు.

- మీ వ్యక్తిగత వివరములను రహస్యముగా ఉంచండి పరిచయములేని వారితో జాగ్రత్త .

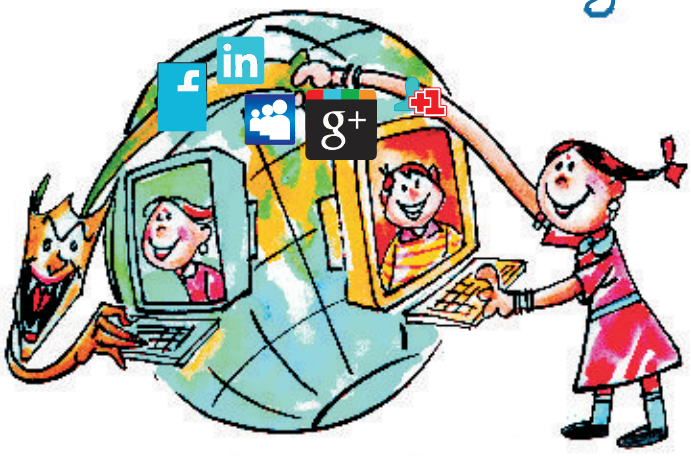
- స్నేహితులు పరిచయస్తులు కాని వ్యక్తులతో స్నేహము కొరకు విన్నపములను మరియు మీ వ్యక్తిగత వివరములను ఇచ్చుటకు తిరస్కరించండి. సంబంధాలు బెడిసినప్పుడు దూషించు మరియు అసభ్యకర సందేశములను పంపవచ్చు.

క్రింది ప్రమాదములతో జాగ్రత్త

స్పామ్:

స్పామ్ అంటే ఏదైన వస్తువు గురించి ను ఇ-మెయిల్‌లిస్టుకు లేదా ఇ-మెయిల్ గ్రూపులకు పంపు అనవసర ఇ-మెయిల్ ప్రకటన లు. అలాగే స్పామర్స్ కూడా అనవసర ఇ-మెయిల్స్ ను ఉచిత సోషల్ నెట్‌వర్కింగ్ సైట్ల ను వినియోగించు కొన్ని బిలియన్ల వినియోగదారులకు, స్పామర్లు సులభంగా వారి వ్యక్తిగత సమాచారమును సేకరించి పంపుచున్నారు.

అప్‌డేట్ చేసిన స్పామ్-బ్లాకింగ్ సాఫ్ట్‌వేర్‌నే ఎల్లప్పుడూ ఉపయోగించండి.



స్కామ్స్:

సాధారనంగా ఆన్ లైన్ స్కామర్స్ , వినియోగదారులను కొత్త ఫోలోవర్సను జత చేసుకొనుటకు వ్యక్తిగత వివరములకై అడుగుచూ లింకుతో ఉన్న ఇ-మెయిల్ లేదా సందేశములను పంపుతారు. ఈ లింకులు అప్లికేషన్స్, గేమ్స్ మొదలగునటువంటి వాటిలాగా ఉంటాయి. ఎప్పుడైనా వినియోగదారుడు తమ వ్యక్తిగత వివరములను ఈ లింకులకు పంపిన వెంటనే స్కామర్స్ ఆ వివరములను తీసుకొని దుర్వినియోగపరచవచ్చు.

హానికర అప్లికేషన్స్:

హానికర అప్లికేషన్స్, వివిధ అప్లికేషన్స్ ను వినియోగించునప్పుడు లేదా సాఫ్ట్‌వేర్ ఇన్స్టలేషన్ అప్పుడు రావచ్చు. అప్లికేషన్ ఇన్స్టలేషన్ మొదలు పెట్టుటకు, లేదా విడియోలను వీక్షించుటకు లింకులు మొదలగు వాటికై సోషల్ నెట్‌వర్కింగ్ అప్లికేషన్స్ పై క్లిక్ చేస్తే , మీరు అడిగిన అప్లికేషన్స్ ను మొదలు పెట్టుటకు మీమౌలిక సమాచారమును, మీ వాల్ అప్ డేట్ , వాల్ పై పోస్టు చేయుటకు వారికి వీలు కల్పించవలసిందిగా అడుగుతూ, ఇటువంటి హానికర అప్లికేషన్స్ రావచ్చు.

క్లిక్ జాకింగ్:

ఇంటర్నెట్ వాడకదారు ప్రమాదరహిత వెబ్‌పేజీలపై క్లిక్ చేస్తున్నసమయంలో వారిని తప్పుదోవ పట్టించి వారి రహస్య సమాచారాన్ని రాబట్టుకోవటం, ఆ కంప్యూటర్‌ను తమ అధీనంలోకి తీసుకోవటం అనేమోసాన్ని క్లిక్ జాకింగ్ అంటారు. అనేక బ్రౌజర్‌లు, ప్లాట్‌ఫామ్‌లు క్లిక్‌జాకింగ్‌కు అనువుగా ఉన్నాయి. వాడకందారుకు తెలియకుండానే నడిచే ఎంబెడెడ్ కోడ్ లేదా స్క్రిప్ట్‌ద్వారా క్లిక్‌జాకింగ్ జరుగుతుంది. ఇది సోషల్‌నెట్‌వర్కింగ్ డొమైన్‌లో కూడా జరుగుతుంటుంది.వాడకదారులతో కొన్ని లింక్‌లు, ఐకాన్‌లు, బటన్‌లు మొదలైనవాటిపై క్లిక్ చేయించటంద్వారా వారికి తెలియకుండా వారే హానికరమైన పనులు చేసేటట్లు చేయటం ఈ చర్యవెనక ఉన్న లక్ష్యం.

ఫిషింగ్:

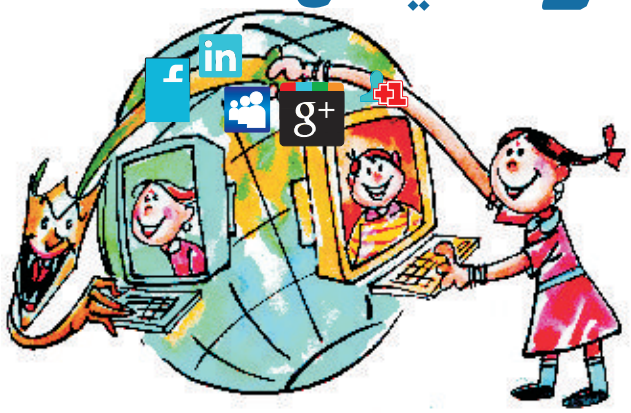
అసలు వెబ్‌సైట్‌లాగానే నకిలీ సైట్‌ను సృష్టించటాన్ని ఫిషింగ్ అంటారన్నది అందరికీ తెలిసిన విషయమే. బ్యాంకులు, సుప్రసిద్ధ వాణిజ్య వెబ్‌సైట్లపై చేసినట్లుగానే సోషల్ నెట్‌వర్కింగ్ లో కూడా ఇప్పుడు ఫిషింగ్ జరుగుతోంది. ప్రత్యేకమైన థీమ్‌లు అందిస్తున్నామని, ప్రొఫైల్ అప్‌డేట్ చేసుకోమని, సెక్యూరిటీ అప్లికేషన్/ఫీచర్స్ అప్‌డేట్ చేసుకోమనితెలుపుతూ బూటకపు ఇ-మెయిల్స్, సందేశాలు పంపటం సోషల్ నెట్‌వర్కింగ్‌లో జరిగే ఫిషింగ్. ఆ అప్‌డేట్స్ చూడటానికి నెట్ వాడకందారు ఒక లింక్‌ను అనుసరించి, లాగిన్ అవ్వాల్సి ఉంటుంది. అప్పుడు వారి వివరాలను మోసగాళ్ళు సేకరిస్తారు. అసలు లాగిన్‌పేజికి నకలుగా సృష్టించబడిన ఆ లింక్‌పేజి రహస్య సమాచారాన్ని సేకరించటానికి ఉద్దేశించబడినది.

ఫిషింగ్ ఇ-మైల్ స్కామ్స్ నుండి అప్రమత్తంగ ఉండండి

మార్గదర్శకాలు

- మీ పేరు, ఇంటి/పాఠశాల చిరునామా, ఫోన్ నంబర్‌లు, వయస్సు, లింగం, క్రెడిట్ కార్డ్ వివరాలు వంటి వ్యక్తిగత సమాచారాన్ని ఎప్పుడు ఇవ్వొద్దు, పోస్ట్ చేయొద్దు.
- ఇంటర్నెట్ అనేది ప్రపంచంలోని అతిపెద్ద సమాచార మార్పిడి సాధనంకాబట్టి మీరు ఆన్‌లైన్‌లో పోస్ట్ చేసే సమాచారాన్ని ఆన్‌లైన్‌లో ఉన్న ప్రతి ఒక్కరూ చూడొచ్చు. మీరు వాడుతున్న వెబ్‌సైట్‌నే వాడే ఇతరులు మీరు పోస్ట్ చేసిన సమాచారాన్ని , మీ ప్రొఫైల్‌ను తెలుసుకోవచ్చు. మీ ఎకౌంటును చూసేవారిలో మీ తల్లిదండ్రులు, స్నేహితులు, టీచర్లువంటి మంచివారితో పాటు అపరిచితులైన చెడ్డవారు కూడా ఉంటారు.
- మీరు వెబ్‌సైట్లలో ఇచ్చిన సమాచారము మిమ్ములను ఇరికించటానికికూడా ఉపయోగపడే అవకాశం ఉన్నదని గుర్తుంచుకోండి.
- మీ పాస్‌వర్డ్ ను మీ తల్లిదండ్రులకు లేదా సంరక్షకులకు తప్ప ఇంకెవరికి ఇవ్వరాదు.
- మీ పాస్‌వర్డ్ ను తరుచుగా మార్చుతూ ఉండండి మరియు తిరిగి సోషల్ నెట్‌వర్కింగ్ సైట్లకు పంపే లింకులపై క్లిక్ చేయకండి. మీరు తిరిగి మీ ఎకౌంటు లోకి వెళ్ళుటకు బ్రౌజర్లలో టైపు చేయండి లేదా మీరు సేవ్ చేసిన బుక్‌మార్క్స్ ను ఉపయోగించండి.
- సోషల్ నెట్‌వర్క సైట్లను ఎన్నుకున్నప్పుడు గోప్య వివాదాస్పద అంశాలను పరిశీలించాలి.
- సోషల్ నెట్‌పర్కింగ్ సైట్లలో స్నేహితులను జత పరుచుకునేటప్పుడు మీకు తెలిసినవారిని మాత్రమే అంగీకరించండి.
- ఎప్పుడూ కూడ సోషల్ నెట్‌వర్కింగ్ సైట్లలో పరిచయమైన వ్యక్తులను వ్యక్తిగతంగా కలవకూడదు. ఎందుకంటే వారు మీకు చెప్పిన విధమైన వ్యక్తులు కాకపోవచ్చు.
- సోషల్ నెట్‌వర్కింగ్ సైట్లలో పరిచయమైన వ్యక్తులను కలిసే ముందు మీ తల్లిదండ్రుల అంగీకారమును పొందండి.
- సోషల్ నెట్‌వర్కింగ్ సైట్లు , వాడకదారులు తమ సమాచారాన్ని ఎవరెవరు చూడొచ్చని నియంత్రించుకోటానికి అవకాశాలు కలిగిస్తున్నాయి. ఈ సౌలభ్యాలను వినియోగించుకోండి.
- మీ కుటుంబ గౌరవాన్ని భంగ పరిచే టాపిక్‌లను రాయకండి.
- సోషల్ నెట్‌వర్కింగ్ సైట్లలో పరిచయములేని వ్యక్తులకు మీ ఫొటోలను, విడియోలను మరే ఇతర సున్నితమైన సమాచారమును పంపవద్దు.
- సోషల్ నెట్‌వర్కింగ్ ఎకౌంటు నుండి మీ సమాచారమును మార్చినా లేక దొంగలించబడినా వెంటనే సోషల్ నెట్‌వర్కింగ్ సపోర్ట్ టీంకు తెలియచేయండి.
- మీ ప్రొఫైల్ లో ఎవరైన పరూషమైన లేదా బాదకలిగించు విధంగా పొస్టులు రాస్తే స్పధించకండి.
- అనవసరమైన విమర్శలను పంపించి స్నేహితులను లేదా సందేశాలను తొలగించి ఈ విమర్శలను నెట్‌వర్కింగ్ సైట్లకు తెలియ చేయండి.
- మీ స్నేహితుల వివరాలను నెట్‌వర్కింగ్ సైట్ల లో పోస్టు చేయకండి. అది వారిని ఇబ్బందికి గురిచేయవచ్చు. వారి గ్రూపు ఫొటోలను, స్కూలు పేరును, చిరునామాలను, వయసు మొదలగునవి పోస్టు చేయకుండా వారిని సంరక్షించండి.
- నెట్‌వర్కింగ్ సైట్ల్‌లో మీరు చేయబోవు పనులను పోస్టు చేయకండి.
- నెట్‌వర్కింగ్ సైట్ల లో ని సెట్టింగులను పరిశీలించి , మీరు స్నేహితులుగా అంగీకరించిన వ్యక్తులు మాత్రమే జతపరుచుకొనేలా సెట్ చేయండి మరియు మీరు స్నేహితులుగా అంగీకరించిన వ్యక్తులు మాత్రమే మీ ప్రొఫైల్ వీక్షించేలా సెట్ చేయండి.

سائبر اسپیس کے معاملات میں لئے جانے والے احتیاطی اقدامات



گھوٹالے

آن لائین دھوکہ باز افراد عام طور پر ایک ای میل یا میسیج ایک لنک کے ساتھ استفاد ہ کنندہ کو بھیجتے ہیں جس میں شخصی معلوماتِ دریافت کرتے ہیں اور بتا تے ہیں کہ اس کے ذریعہ دوسرے نئے صارفین کو شامل کیا جائے گا۔ یہ جو لنک استفادہ کنندہ کو بھیجتے ہیں یہ اپلکیشن کے مماثل ہوگا یا پھر کیمس وغیرہ کے۔ تو جب کبھی استفادہ کنندہ اپنی تفصیلات اس لنک میں بھیجتا ہے فوری وہ ساری تفصیل ان دھوکہ باز اسکامرس کو پہونچ جاتی ہے جس سے وہ اس کا ناجائز استعمال کر بیٹھتے ہیں۔

مالیشیز اپلکیشنس

مالیشیز اپلکیشن سافٹ ویر کے انسٹال کرنے یا استعمال کرنے کے دوران مختلف اپلکیشنز کے ذریعہ وجود میں آسکتے ہیں۔ اسی طرح، سوشل نیٹ ورکنگ سائیٹ پر کلک کرتے ہی ا پڈیشن کو انسٹال کرنے کا طریقہ شر ع ہوجاتا ہے یا پھر ویڈ یو دیکھنے کا کوئی لنک وغیرہ دیا جاتا ہے۔ اس پر اپنی رضامندی ظاہر کرنے پر آپریشن مکمل کرنے کے لئے درخواست کی جاتی ہے کہ استفادہ کنندہ کی جانب سے کچھ تعمیراتی عمل ہو جیسے بنیادی معلومات فراہم کرنا، وال کو تازہ ترین بنانا، یا میری وال پر پوسٹ کر وکہنا وغیرہ۔

جیکنگ کلک

عام طور پر، جیکنگ کلک ایک بد نیتی پر مبنی ایک ٹیکنک ہے جو کہ ویب استفادہ کنندوں کو ڈھونڈ نکالتی ہے جس میں وہ اپنی خفیہ معلومات کو بیان کرتے ہیں یا ان کے کمپیوٹروں کو مکمل قابو میں کر لیتے ہیں جب کہ وہ معصوم لگنے والے ویب پیجوں پر کلک کرتے ہیں مختلف قسم کے مروزروں اور پلاٹ فارمس کے اطراف خطرات ہوتے ہیں، جیکنگ کا ایک کلک ایک مضبوط کوڈ یا اسکرپٹ کی شکل میں بیٹھ جاتا ہے جو کہ استفادہ کنندہ کو معلوم ہوئے بغیر چل سکتا ہے۔ اسی طرح یہ سوشل نیٹ ورکنگ ڈومین پر بھی لاگو ہوتا ہے۔ اس طرح کے پوشیدہ حملوں کا مقصد یہ ہوتا ہے کہ استفادہ کنندہ اس لکس، ایکانس، بٹنس وغیرہ کو کلک کرتے ہیں پکڑا جاتا ہے، جس سے کہ ایک ٹرگر دب کر دھوکہ دہی کا عمل پیچھے سے پوشیدہ چلنا شروع ہوجاتا ہے جو کہ استفادہ کنندہ کو معلوم نہیں ہوتا۔

- **کسی بھی قیمت پر اپنی شخصی تفصیلات نہ دیں:**
آن لائین پر اپنی ذاتی تفصیلات کو پوسٹ نہ کریں، جیسا کہ آپ کے سفر کی تاریخ، جگہ اور فلم وغیرہ دیکھنے کا وقت جو آپ نے سوچ رکھا ہے۔ شام کے کلاسس جو آپ لیتے ہیں وغیرہ وغیرہ۔

- **رابطہ کی تفصیلات ہمیشہ رازداری میں رکھیں**
: اجنبیوں سے ہوشیار

- **دوست** : اجنبیوں کو دوست بنانے سے پرہیز کرنا بہتر ہے جب کہ ان کی جانب سے دوستی کی دعوت دی جارہی ہو۔

- آپ اپنی پروفائل تفصیلات میں اپنی ذاتی اطلاعات شیئر نہ کریں تعلقات کی صورت میں لاپرواہ عناصر آپ کو گندے/غیر اخلاقی پیامات آپ کو بھیج سکتے ہیں۔

مندرجہ ذیل خطرات سے ہوشیار رہیں

اسپام

جیسا کہ ہم سب بخوبی جانتے ہیں کہ عام طور پر اسپام میں ان چاہے ای میل مختلف پروڈ کٹس کی متعلق تشہیر کے لئے ایک ساتھ بہت سارے ای میلس کو یا پھر ای میل اڈریس کے کروپ کو بھیج دیئے جاتے ہیں۔ اسی طرح اسپامرس ان چاہے میلس یا پیامات کو سوشل نیٹ ورکنگ سائٹس کے کروڑ صارفین کو ایک ساتھ بھیج دیتے ہیں جو کہ مفت ہے اور دھوکہ بازوں کو غیر متعلقہ اشخاص کی ذاتی معلومات حاصل کرنے کا آسان ذریعہ بھی۔

ہمیشہ تازہ ترین اسپام بلا کنگ سافٹ وئیر کا استعمال کریں

- جب آپ کوئی بھی سوشل نیٹ ورکنگ سائیٹ کھولیں، اس کی پرائیویسی یعنی راز داری کے اصول کو اچھی طرح جان لینا چاہیے
- سوشل نیٹ ورکنگ سائیٹ (سماجی رابطہ سائیٹس) پر دوستوں کی دعوت قبول کرنے کے دوران محتاط رہیں۔ صرف ان لوگوں کو بطور دوست بنا کر اپنی سائیٹ میں رکھیں جن کو اپنی حقیقی زندگی میں جانتے ہیں۔
- سوشل نیٹ ورکنگ سائیٹ پر ملنے والے ہر کسی سے شخصی طور پر حقیقی ملاقات نہ کریں کیونکہ ان میں سے چند وہ نہیں ہوتے جو وہ کہتے ہیں
- اگر آپ سوشل نیٹ ورکنگ سائیٹ پر ملے کسی شخص سے ملنا چاہتے ہیں تو آپ اپنے سرپرستوں کی اجازت ضرور لیں
- بہت سارے سوشل نیٹ ورکنگ ویب سائیٹس صارفین کو راز داری کنٹرول میں رکھنے کی سہولت دیتے ہیں جس سے کہ ان سے بچا سکے جو اطلاعات کو دیکھنے کی صلاحیت رکھتے ہیں۔ لہذا اس جیسے سہولیات کو استعمال کریں۔
- کوئی ایسی چیز سائیٹ پر نہ بھیجیں جس سے آپ کے گھر والوں کی شان میں نقصان ہو۔
- سوشل نیٹ ورکنگ سائیٹس پر کسی بھی اجنبی کو فوٹو گرافس، ویڈیو اور کوئی دوسری حساس معلومات بالکل نہ بھیجیں
- اگر آپ کو ایسا لگے کہ سوشل نیٹ ورکنگ سائیٹ پر آپ کا اکاؤنٹ سمجھوتہ یا چوری ہو گیا ہے، تو فوراً نیٹ ورکنگ سائیٹ سپورٹ ٹیم کے ذمہ داران کو فوری رپورٹ کریں
- آپ کے پروفائیل پر پوسٹ کئے گئے غیر اخلاقی اور ہراساں کرنے والے تبصروں کا جواب نہ دیں
- آپ کو متعدد بار غیر مناسب تبصرہ پوسٹ کرنے والے کسی بھی ان چاہے پیام یا پھر دوست کو خارج کر دیں اور ان تبصروں کی رپورٹ فوری طور پر نیٹ ورکنگ سائیٹس کو دیں۔
- آپ اپنے کسی بھی دوست کی اطلاع نیٹ ورکنگ سائیٹس پر نہ دیں، جو کہ انہیں کسی خطرہ میں ڈال سکتا ہے۔ اپنے دوستوں کو گروپ فوٹوز، اسکول کا نام، مقام، عمر، جنس وغیرہ کی اطلاع پوسٹ کرنے سے بچائیں۔
- اپنے پلانس اور کارکردگیوں کی رپورٹ پوسٹ نہ کریں جو نیٹ ورکنگ سائیٹس میں آپ کرنے جا رہے ہیں
- سوشل نیٹ ورکنگ سائیٹس کی پرائیویسی سیٹنگ (یعنی راز داری ترتیب) کی جانچ کر لیں اور اس طرح سیٹ کریں کہ اگر آپ کسی کے ساتھ شامل ہونے پر رضامند ہوں تو وہ لوگ آپ کو صرف بطور دوست شامل کر سکیں اور اس طرح سے بھی سیٹنگ بھی کریں کہ لوگ صرف آپ کی پروفائیل دیکھیں جب کہ آپ اس کو اپنا دوست بنا لے۔

فائشنگ

جیسا کہ ہم سبھی جانتے ہیں کہ فائشنگ حملہ نقلی ویب سائیٹ کی دین ہوتی ہے جو کہ اصلی ویب سائٹ کی قریب قریب ہم شکل ہوتی ہے۔ اسی طرح ان دنوں یہاں تک کہ سوشل نیٹ ورکنگ بھی مختلف رنگ و روپ میں جیسا کہ وہ بینک اور مشہور تجارتی ویب سائیٹس پر فائشنگ کا شکار ہیں۔ سوشل نیٹ ورکنگ فائشنگ نقلی میلس اور پیامات جیسا کہ کچھ مخصوص تھیمس کی پیشکش کرنا، پروفائل کی تجدید کرنا، سیکوریٹی اپلکیشن کی تجدید/خصوصیات وغیرہ۔ تجدید کرنے کے لئے استفادہ کنندہ کو ایک لنک پر عمل آوری کی ضرورت پڑتی ہے اور لاگ ان کرنا پڑتا ہے، جس کے ذریعہ وہ حملہ آور اسنادات لے لیتے ہیں۔ وہ لنک پیج، اصلی لاگن پیج کی نقلی کاپی ہوتی ہے، جس کی مرکزی توجہ استفادہ کنندہ کے کھاتے سے وہ اسنادات کو چرانا ہوتا ہے۔

فائشنگ ای میل اسکامس سے ہوشیار رہیں

ہدایات

- **کوئی بھی ذاتی معلومات جیسا کہ آپ کا نام، اپنے گھر کا یا اسکول کا پتہ، فون نمبرس، عمر، جنس، کریڈٹ کارڈس وغیرہ کی تفصیلات نہ ہی دیں اور نا ہی پوسٹ کریں۔**
- وہ اطلاعات جو آپ نے آن لائین پر پوسٹ کی تھی کوئی بھی کہیں بھی دیکھ سکتا ہے کیونکہ انٹرنیٹ دنیا کا سب سے بڑا معلوماتی تبادلہ کا آلہ ہوتا ہے۔ بہت سارے لوگ جو ویب سائٹ استعمال کرنا جانتے ہیں وہ آپ کے پروفائیل کو دیکھ کر آپ نے جو تفصیلات پوسٹ کی وہ ساری معلومات بآسانی حاصل کر لیتے ہیں۔ وہ افراد جو کہ آپ کی پروفائیل کو ایکسس کرنے کی رسائی رکھتے ہیں ان میں ہر کوئی شامل ہے جیسے اچھے اشخاص میں آپ کے دوست، سرپرست، اساتذہ ہیں اور برے لوگ جیسے اجنبی افراد۔
- **ہوشیار رہیں کہ جو اطلاعات آپ ان سائٹس پر دیتے ہیں وہ آپ کو نشانہ بنا کر خطرہ میں بھی ڈال سکتے ہیں**
- آپ اپنا پاس ورڈ اپنے سرپرست یا ذمہ داران کے علاوہ کسی کو بھی نہ دیں آپ اپنا پاس ورڈ بار بار بدلاتے رہیں، اور لنکس کو کلک کرنے سے بچتے رہیں جو آپ کو واپس سوشل نیٹ ورک سائٹ پر پہچانے کا کام کرتے ہیں، اس کی جگہ، آپ سائٹ کا ایڈرس صاف صاف اپنے بروزر میں ٹائپ کریں (یا پھر بک مارک بنا کر محفوظ کر لیں جو آپ نے محفوظ Save کیا ہے) تا کہ آپ اپنے کھاتے میں پہونچ جائیں۔