Question Bank

**సైబర్ పరిశుభ్రత**

ప్రశ్న 1: సైబర్ పరిశుభ్రత అంటే ఏమిటి?

ఎ) మీ కంప్యూటర్‌ను భౌతికంగా శుభ్రపరచడం.

బి) ఇంటర్నెట్‌ని ఉపయోగిస్తున్నప్పుడు వ్యక్తిగత పరిశుభ్రతను పాటించడం.

సి) ఆన్‌లైన్ భద్రత మరియు భద్రతను నిర్ధారించడానికి పద్ధతులను అమలు చేయడం.

డి) డిజిటల్ పరికరాలకు సంబంధించిన వైద్య పరిస్థితి.

సమాధానం: సి) ఆన్‌లైన్ భద్రత మరియు భద్రతను నిర్ధారించడానికి పద్ధతులను అమలు చేయడం.

ప్రశ్న 2: సైబర్ పరిశుభ్రత కోసం కింది వాటిలో ఏది మంచి పాస్‌వర్డ్ అభ్యాసం?

ఎ) బహుళ ఖాతాల కోసం ఒకే పాస్‌వర్డ్‌ను ఉపయోగించడం.

బి) పుట్టిన తేదీల వంటి వ్యక్తిగత సమాచారం ఆధారంగా పాస్‌వర్డ్‌లను సృష్టించడం.

సి) అక్షరాలు, సంఖ్యలు మరియు ప్రత్యేక అక్షరాల కలయికతో పొడవైన మరియు సంక్లిష్టమైన పాస్‌వర్డ్‌లను ఉపయోగించడం.

D) సులభంగా యాక్సెస్ కోసం పాస్‌వర్డ్‌లను కాగితంపై రాయడం.

సమాధానం: సి) అక్షరాలు, సంఖ్యలు మరియు ప్రత్యేక అక్షరాల కలయికతో పొడవైన మరియు సంక్లిష్టమైన పాస్‌వర్డ్‌లను ఉపయోగించడం.

ప్రశ్న 3: సాఫ్ట్‌వేర్ మరియు అప్లికేషన్‌లను క్రమం తప్పకుండా అప్‌డేట్ చేయడం వల్ల ప్రయోజనం ఏమిటి?

ఎ) సాఫ్ట్‌వేర్ వేగంగా పని చేయడానికి.

బి) కొత్త ఫీచర్లు మరియు ఫంక్షనాలిటీలను జోడించడానికి.

సి) యూజర్ ఇంటర్‌ఫేస్‌ని మెరుగుపరచడానికి.

డి) భద్రతా లోపాలను సరిచేయడానికి మరియు బగ్‌లను సరిచేయడానికి.

సమాధానం: D) భద్రతా లోపాలను సరిచేయడానికి మరియు బగ్‌లను పరిష్కరించడానికి.

ప్రశ్న 5: ఇమెయిల్‌లు లేదా సందేశాలలోని లింక్‌లపై క్లిక్ చేసేటప్పుడు మీరు ఎందుకు జాగ్రత్తగా ఉండాలి?

ఎ) లింక్‌లపై క్లిక్ చేయడం వల్ల మీ ఇంటర్నెట్ కనెక్షన్ నెమ్మదించవచ్చు.

బి) లింక్‌లపై క్లిక్ చేయడం వల్ల అవాంఛిత డౌన్‌లోడ్‌లకు దారితీయవచ్చు.

సి) లింక్‌లు మాల్వేర్‌ను కలిగి ఉండవచ్చు లేదా ఫిషింగ్ కోసం ఉపయోగించే నకిలీ వెబ్‌సైట్‌లకు నేరుగా పంపవచ్చు.

డి) లింక్‌లపై క్లిక్ చేయడం కాపీరైట్ చట్టాలను ఉల్లంఘించవచ్చు.

సమాధానం: సి) లింక్‌లు మాల్వేర్‌ను కలిగి ఉండవచ్చు లేదా ఫిషింగ్ కోసం ఉపయోగించే నకిలీ వెబ్‌సైట్‌లకు నేరుగా పంపవచ్చు.

ప్రశ్న 6: మీరు ఇంటర్నెట్ ద్వారా సురక్షితమైన డేటా ప్రసారాన్ని ఎలా నిర్ధారించగలరు?

A) సున్నితమైన లావాదేవీల కోసం పబ్లిక్ Wi-Fi నెట్‌వర్క్‌లను ఉపయోగించడం.

బి) ఎన్‌క్రిప్ట్ (Encrypt) చేయని ఇమెయిల్ ద్వారా వ్యక్తిగత సమాచారాన్ని పంపడం.

సి) వెబ్‌సైట్‌లు URLలో "HTTPS"కి బదులుగా "HTTP"ని కలిగి ఉన్నాయని నిర్ధారించుకోవడం.

D) ఆన్‌లైన్ కార్యకలాపాల కోసం HTTPS వంటి సురక్షితమైన మరియు గుప్తీకరించిన కనెక్షన్‌లను ఉపయోగించడం.

సమాధానం: D) ఆన్‌లైన్ కార్యకలాపాల కోసం HTTPS వంటి సురక్షితమైన మరియు గుప్తీకరించిన కనెక్షన్‌లను ఉపయోగించడం.

ప్రశ్న 7: మీ డేటాను క్రమం తప్పకుండా బ్యాకప్ చేయడం వల్ల ప్రయోజనం ఏమిటి?

ఎ) ఇంటర్నెట్ బ్యాండ్‌విడ్త్ వినియోగాన్ని తగ్గించడానికి.

బి) మీ పరికరంలో నిల్వ స్థలాన్ని ఖాళీ చేయడానికి.

సి) హార్డ్‌వేర్ వైఫల్యం, సైబర్ సంఘటనలు లేదా ప్రమాదాలు సంభవించినప్పుడు డేటా నష్టం నుండి రక్షించడానికి.

D) మీ పరికరం పనితీరును మెరుగుపరచడానికి.

సమాధానం: సి) హార్డ్‌వేర్ వైఫల్యం, సైబర్ సంఘటనలు లేదా ప్రమాదాలు సంభవించినప్పుడు డేటా నష్టం నుండి రక్షించడానికి.

ప్రశ్న 8: సైబర్ పరిశుభ్రత విషయంలో ఫైర్‌వాల్ అంటే ఏమిటి?

ఎ) భౌతిక పరికరాలను భద్రపరచడానికి ఉపయోగించే రక్షణ అవరోధం.

బి) కంప్యూటర్ లోపల హార్డ్‌వేర్ భాగం.

సి) సైబర్ బెదిరింపును నిరోధించడానికి ఉపయోగించే పరికరం.

D) నెట్‌వర్క్ ట్రాఫిక్‌ను ఫిల్టర్ చేసే మరియు అనధికారిక యాక్సెస్‌ను నిరోధించే భద్రతా వ్యవస్థ.

సమాధానం: D) నెట్‌వర్క్ ట్రాఫిక్‌ను ఫిల్టర్ చేసే భద్రతా వ్యవస్థ మరియు అనధికార యాక్సెస్‌ను బ్లాక్ చేస్తుంది.

ప్రశ్న 9: షేర్డ్ కంప్యూటర్‌లలో ఖాతాల నుండి లాగ్ అవుట్ చేయడం ఎందుకు కీలకం?

ఎ) మాల్వేర్ ఇన్ఫెక్షన్ నుండి రక్షించడానికి.

బి) డిజిటల్ పాదముద్రను వదిలివేయకుండా ఉండటానికి.

సి) మీ ఖాతాలు మరియు వ్యక్తిగత సమాచారానికి అనధికార ప్రాప్యతను నిరోధించడానికి.

D) షేర్డ్ కంప్యూటర్‌లో బ్యాటరీ శక్తిని ఆదా చేయడానికి.

సమాధానం: సి) మీ ఖాతాలు మరియు వ్యక్తిగత సమాచారానికి అనధికారిక యాక్సెస్‌ను నిరోధించడానికి.

ప్రశ్న 10: మీ పరికరాలను సురక్షితంగా ఉంచడానికి కింది వాటిలో ఏది సిఫార్సు చేయబడిన సైబర్ పరిశుభ్రత అభ్యాసం?

ఎ) అనధికారిక వెబ్‌సైట్ల నుండి సాఫ్ట్‌వేర్ మరియు అప్లికేషన్‌లను డౌన్‌లోడ్ చేయడం.

బి) ప్రక్రియపై మరింత నియంత్రణను కలిగి ఉండటానికి ఆటోమేటిక్ సాఫ్ట్‌వేర్ నవీకరణలను నిలిపివేయడం.

సి) మీ పరికరాలను ఛార్జ్ చేయడానికి పబ్లిక్ USB ఛార్జింగ్ పోర్ట్‌లను ఉపయోగించడం.

డి) ప్రసిద్ధ యాంటీవైరస్ మరియు యాంటీ మాల్వేర్ సాఫ్ట్‌వేర్‌లను ఇన్‌స్టాల్ చేయడం.

సమాధానం: D) ప్రసిద్ధ యాంటీవైరస్ మరియు యాంటీ మాల్వేర్ సాఫ్ట్‌వేర్‌లను ఇన్‌స్టాల్ చేయడం.

**నెటికెట్లు**

నెటికెట్ దేనిని సూచిస్తుంది?

ఎ) ఇంటర్నెట్‌లో మర్యాదపూర్వకమైన మరియు గౌరవప్రదమైన ప్రవర్తనకు సంబంధించిన నియమాలు మరియు సమావేశాలు.

బి) కొత్త నెట్‌వర్క్ మౌలిక సదుపాయాలను సృష్టించే ప్రక్రియ.

సి) ఆన్‌లైన్‌లో వ్యక్తిగత డేటాను భద్రపరిచే అభ్యాసం.

D) ఇంటర్నెట్ వినియోగాన్ని పర్యవేక్షించడానికి ఒక సాఫ్ట్‌వేర్ సాధనం.

జవాబు: ఎ) ఇంటర్నెట్‌లో మర్యాదపూర్వకమైన మరియు గౌరవప్రదమైన ప్రవర్తనకు సంబంధించిన నియమాలు మరియు సమావేశాలు.

ప్రశ్న 2: ఆన్‌లైన్ కమ్యూనికేషన్‌లో అన్ని పెద్ద అక్షరాలను ఉపయోగించడం ఎప్పుడు సముచితం?

ఎ) ముఖ్యమైన అంశాలను నొక్కి చెప్పడం లేదా ఉత్సాహాన్ని వ్యక్తం చేయడం.

బి) పూర్తి సందేశం లేదా ఇమెయిల్ రాయడానికి.

సి) ఆన్‌లైన్‌లో ఇతరులను చికాకు పెట్టడం మరియు బాధించడం.

డి) అనామక ఫోరమ్‌లలో ఒకరి గుర్తింపును దాచడం.

జవాబు: ఎ) ముఖ్యమైన అంశాలను నొక్కి చెప్పడం లేదా ఉత్సాహాన్ని వ్యక్తం చేయడం.

ప్రశ్న 3: ఆన్‌లైన్ విమర్శలు లేదా ప్రతికూల వ్యాఖ్యలకు ప్రతిస్పందించడానికి ఉత్తమ మార్గం ఏమిటి?

ఎ) వ్యాఖ్యలను విస్మరించండి మరియు అవి ఉనికిలో లేనట్లు నటించండి.

బి) దూకుడు భాష మరియు అవమానాలతో ప్రతిస్పందించండి.

సి) గౌరవప్రదమైన మరియు నిర్మాణాత్మక సంభాషణలో పాల్గొనండి.

డి) వ్యాఖ్యలను తొలగించండి మరియు వ్యక్తిని బ్లాక్ చేయండి.

సమాధానం: సి) గౌరవప్రదమైన మరియు నిర్మాణాత్మక సంభాషణలో పాల్గొనండి.

ప్రశ్న 4: ఆన్‌లైన్ కమ్యూనికేషన్‌లో ఎమోజీలు మరియు ఎమోటికాన్‌లను ఉపయోగించడం వల్ల ప్రయోజనం ఏమిటి?

ఎ) పదాలు మరియు వాక్యాలను భర్తీ చేయడానికి.

బి) సందేశానికి హాస్యం మరియు వ్యక్తిత్వాన్ని జోడించడం.

సి) గ్రహీతను గందరగోళానికి గురిచేయడం.

D) స్థలం మరియు సమయాన్ని ఆదా చేయడానికి.

సమాధానం: బి) సందేశానికి హాస్యం మరియు వ్యక్తిత్వాన్ని జోడించడానికి.

ప్రశ్న 5: ఆన్‌లైన్‌లో వ్యక్తిగత సమాచారాన్ని పంచుకోవడం ఎప్పుడు సముచితం?

ఎ) ఎప్పుడైనా, అడిగే వ్యక్తిని మీరు విశ్వసించినంత కాలం.

బి) సన్నిహిత స్నేహితులు మరియు కుటుంబ సభ్యులతో మాత్రమే.

సి) దీన్ని ఎప్పుడూ చేయకండి, ఎందుకంటే ఇది హానికరమైన ప్రయోజనాల కోసం ఉపయోగించబడుతుంది.

డి) కఠినమైన గోప్యతా సెట్టింగ్‌లతో సోషల్ మీడియా ప్రొఫైల్‌లలో మాత్రమే.

సమాధానం: సి) ఎప్పుడూ, ఇది హానికరమైన ప్రయోజనాల కోసం ఉపయోగించబడవచ్చు.

ప్రశ్న 6: ఆన్‌లైన్ చర్చలు లేదా ఫోరమ్‌లలో మీరు విభేదాలు లేదా వైరుధ్యాలను ఎలా నిర్వహించాలి?

ఎ) సంభాషణను నివారించండి మరియు చర్చను వదిలివేయండి.

బి) వాదనను గెలవడానికి వ్యక్తిగత దాడులకు పాల్పడండి.

సి) గౌరవప్రదంగా ఉండండి మరియు మీ దృక్కోణానికి మద్దతు ఇవ్వడానికి సాక్ష్యాలను సమర్పించండి.

డి) వేధింపుల కోసం వ్యతిరేక అభిప్రాయాలు ఉన్న వ్యక్తిని నివేదించండి.

సమాధానం: సి) గౌరవప్రదంగా ఉండండి మరియు మీ దృక్కోణానికి మద్దతు ఇవ్వడానికి సాక్ష్యాలను సమర్పించండి.

ప్రశ్న 7: ఆన్‌లైన్‌లో వేరొకరు సృష్టించిన కంటెంట్‌ను భాగస్వామ్యం చేయడానికి ముందు మీరు ఏమి పరిగణించాలి?

ఎ) క్రెడిట్ ఇవ్వకుండా షేర్ చేయండి, ఇది ఇప్పటికే పబ్లిక్‌గా ఉంది.

బి) అసలు సృష్టికర్త నుండి అనుమతి కోసం అడగండి.

సి) కంటెంట్‌ని ఎడిట్ చేయండి మరియు దానిని మీ స్వంతంగా క్లెయిమ్ చేయండి.

డి) ఏవైనా సమస్యలు రాకుండా అనామకంగా షేర్ చేయండి.

సమాధానం: బి) అసలు సృష్టికర్త నుండి అనుమతి కోసం అడగండి.

ప్రశ్న 8: గ్రూప్ చాట్‌లు లేదా ఫోరమ్‌లలో పాల్గొనేటప్పుడు కింది వాటిలో ఏది మంచి నెటికెట్‌గా పరిగణించబడుతుంది?

ఎ) సంబంధం లేని మరియు ఆఫ్-టాపిక్ కంటెంట్‌ను పోస్ట్ చేయడం.

బి) సంభాషణను విస్మరించడం మరియు సహకరించకపోవడం.

సి) స్పష్టమైన మరియు వివరణాత్మక సబ్జెక్ట్ లైన్లను ఉపయోగించడం.

డి) ప్రతి సందేశానికి "నేను అంగీకరిస్తున్నాను" లేదా "నేను కూడా" అని ప్రతిస్పందించడం.

సమాధానం: సి) స్పష్టమైన మరియు వివరణాత్మక సబ్జెక్ట్ లైన్లను ఉపయోగించడం.

ప్రశ్న 9: మీరు పొరపాటున తప్పు గ్రహీతకు ఇమెయిల్ పంపితే మీరు ఏమి చేయాలి?

ఎ) విస్మరించండి, ఎందుకంటే మీరు ఏమీ చేయలేరు.

బి) ఇమెయిల్‌ను వెంటనే తొలగించమని స్వీకర్తను అడగండి.

సి) తప్పు గురించి గ్రహీతకు తెలియజేయండి మరియు క్షమాపణ చెప్పండి.

D) సంఘటనను ఇమెయిల్ ప్రొవైడర్‌కు నివేదించండి.

సమాధానం: సి) తప్పు గురించి గ్రహీతకు తెలియజేయండి మరియు క్షమాపణ చెప్పండి.

ప్రశ్న 10: ఆన్‌లైన్ పరస్పర చర్యలలో ఎవరైనా మొరటుగా లేదా అభ్యంతరకరంగా ప్రవర్తించినప్పుడు మీరు ఎలా వ్యవహరించాలి?

ఎ) మిమ్మల్ని మీరు రక్షించుకోవడానికి ఇలాంటి ప్రవర్తనలో పాల్గొనండి.

బి) వ్యక్తిని బహిరంగంగా ఎదుర్కోవడం మరియు వారిని అవమానించడం.

సి) వ్యక్తిని విస్మరించండి మరియు ఎటువంటి ప్రతిస్పందనను నివారించండి.

డి) అభ్యంతరకరమైన ప్రవర్తనను ఆపమని వ్యక్తిని మర్యాదపూర్వకంగా అడగండి.

జవాబు: డి) అభ్యంతరకరమైన ప్రవర్తనను ఆపమని మర్యాదపూర్వకంగా వ్యక్తిని అడగండి.

**ఆన్‌లైన్ తరగతుల మర్యాదలు:**

ప్రశ్న 1: "ఆన్‌లైన్ తరగతుల మర్యాదలు" దేనిని సూచిస్తాయి?

ఎ) ఆన్‌లైన్ తరగతులకు సరైన డ్రెస్ కోడ్.

బి) వర్చువల్ లెర్నింగ్ సమయంలో మర్యాదపూర్వకమైన మరియు గౌరవప్రదమైన ప్రవర్తన కోసం ప్రవర్తనలు మరియు మార్గదర్శకాలు.

సి) ఆన్‌లైన్ తరగతుల సమయంలో ఇంటర్నెట్ కనెక్షన్‌ని మెరుగుపరచడానికి సాంకేతికతలు.

డి) ఆన్‌లైన్ తరగతులకు హాజరైనప్పుడు బహువిధి కోసం చిట్కాలు.

జవాబు: బి) వర్చువల్ లెర్నింగ్ సమయంలో మర్యాదపూర్వకమైన మరియు గౌరవప్రదమైన ప్రవర్తన కోసం ప్రవర్తనలు మరియు మార్గదర్శకాలు.

ప్రశ్న 2: ఆన్‌లైన్ తరగతులకు సకాలంలో చేరడం ఎందుకు అవసరం?

ఎ) ముఖ్యమైన ప్రకటనలు మరియు సూచనలను కోల్పోకుండా ఉండటానికి.

బి) తరగతి ప్రారంభమయ్యే ముందు స్నేహితులతో ఎక్కువ సమయం గడపడం.

సి) ఇతర కార్యకలాపాలకు అదనపు సమయాన్ని కేటాయించడం.

డి) తరగతి సమయంలో అంతరాయాలను నివారించడానికి.

జవాబు: ఎ) ముఖ్యమైన ప్రకటనలు మరియు సూచనలను కోల్పోకుండా ఉండటానికి.

ప్రశ్న 3: ఆన్‌లైన్ తరగతుల సమయంలో మీరు మీ టీచర్ లేదా బోధకుడిని ఎలా సంబోధించాలి?

ఎ) స్నేహపూర్వక వాతావరణాన్ని సృష్టించడానికి వారి మొదటి పేరును ఉపయోగించడం.

బి) గౌరవం చూపించడానికి వారి పూర్తి పేరుతో వారిని సూచించడం.

సి) వారి టైటిల్ మరియు ఇంటిపేరును ఉపయోగించడం (ఉదా., మిస్టర్ స్మిత్ లేదా శ్రీమతి జాన్సన్).

D) ఫార్మాలిటీని నిర్వహించడానికి నేరుగా వారిని సంబోధించడం మానుకోండి.

సమాధానం: సి) వారి టైటిల్ మరియు ఇంటిపేరును ఉపయోగించడం (ఉదా., మిస్టర్ స్మిత్ లేదా శ్రీమతి జాన్సన్).

ప్రశ్న 4: మీరు ఆన్‌లైన్ క్లాస్ సమయంలో సాంకేతిక సమస్యలను ఎదుర్కొంటే తగిన చర్య ఏమిటి?

ఎ) సమస్యలను విస్మరించి, తరగతికి హాజరుకావడం కొనసాగించండి.

బి) సమస్య గురించి మీ ఉపాధ్యాయులకు మరియు IT విభాగానికి తెలియజేయండి.

సి) తరగతి నుండి వెంటనే లాగ్ అవుట్ చేసి, తర్వాత మళ్లీ చేరండి.

డి) సమస్యలను మీరే పరిష్కరించుకోవడానికి ప్రయత్నించండి.

సమాధానం: బి) సమస్య గురించి మీ ఉపాధ్యాయులకు మరియు IT విభాగానికి తెలియజేయండి.

ప్రశ్న 5: ఆన్‌లైన్ క్లాస్‌లో మీరు మాట్లాడనప్పుడు మీ మైక్రోఫోన్‌ను మ్యూట్ చేయడం ఎందుకు అవసరం?

ఎ) నేపథ్య శబ్దం తరగతికి అంతరాయం కలిగించకుండా నిరోధించడానికి.

బి) మీ పరికరంలో బ్యాటరీ జీవితాన్ని ఆదా చేయడానికి.

సి) తరగతి వెలుపల ఇతరులకు వినిపించకుండా ఉండటానికి.

డి) తరగతి చర్చపై మీ దృష్టిని పెంచడానికి.

సమాధానం: A) తరగతికి అంతరాయం కలిగించకుండా నేపథ్య శబ్దాన్ని నిరోధించడానికి.

ప్రశ్న 6: మీరు ఆన్‌లైన్ క్లాస్ చర్చలు లేదా ప్రశ్నోత్తరాల సెషన్‌లలో ఎలా పాల్గొనాలి?

ఎ) మీ ఆలోచనలను పంచుకోవడానికి ఉపాధ్యాయుడిని లేదా ఇతర విద్యార్థులను అంతరాయం కలిగించండి.

బి) మాట్లాడే ముందు ఉపాధ్యాయుడు మిమ్మల్ని పిలవడానికి వేచి ఉండండి.

సి) చర్చల సమయంలో గోప్యతను నిర్ధారించడానికి మృదువుగా మాట్లాడండి.

డి) మీ చేతిని పైకెత్తండి లేదా ప్రశ్నలు అడగడానికి లేదా సహకరించడానికి చాట్ ఫీచర్‌ని ఉపయోగించండి.

సమాధానం: D) మీ చేతిని పైకెత్తండి లేదా ప్రశ్నలు అడగడానికి లేదా సహకరించడానికి చాట్ ఫీచర్‌ని ఉపయోగించండి.

ప్రశ్న 7: ఆన్‌లైన్ తరగతుల సమయంలో ఇంటర్నెట్ వినియోగం కోసం ఉత్తమమైన అభ్యాసం ఏమిటి?

ఎ) చిన్న విరామాల కోసం సోషల్ మీడియా మరియు ఎంటర్‌టైన్‌మెంట్ వెబ్‌సైట్‌లను యాక్సెస్ చేయడం.

బి) అంతరాయాలను నివారించడానికి నమ్మకమైన మరియు స్థిరమైన ఇంటర్నెట్ కనెక్షన్‌ని ఉపయోగించడం.

సి) తరగతికి హాజరవుతున్నప్పుడు బ్యాక్‌గ్రౌండ్‌లో పెద్ద ఫైల్‌లను డౌన్‌లోడ్ చేయడం.

D) తరగతి విరామ సమయంలో ఇమెయిల్‌లను తనిఖీ చేయడం మరియు సందేశాలకు ప్రత్యుత్తరం ఇవ్వడం.

సమాధానం: బి) అంతరాయాలను నివారించడానికి విశ్వసనీయ మరియు స్థిరమైన ఇంటర్నెట్ కనెక్షన్‌ని ఉపయోగించడం.

ప్రశ్న 8: ఆన్‌లైన్ తరగతుల సమయంలో మీరు కుటుంబ సభ్యులు లేదా పెంపుడు జంతువుల నుండి పరధ్యానాన్ని ఎలా నిర్వహించాలి?

ఎ) నిశ్శబ్ద వాతావరణాన్ని కొనసాగించడానికి వెంటనే వాటిని మానేయండి.

బి) వాటిని విస్మరించండి మరియు తరగతిపై మాత్రమే దృష్టి పెట్టండి.

సి) పరధ్యానం గురించి మీ గురువుకు మర్యాదపూర్వకంగా తెలియజేయండి మరియు అవసరమైతే క్లుప్తంగా దూరంగా ఉండండి.

డి) తరగతికి అంతరాయం కలిగించినందుకు కుటుంబ సభ్యులు లేదా పెంపుడు జంతువులను శిక్షించండి.

సమాధానం: సి) పరధ్యానం గురించి మర్యాదపూర్వకంగా మీ గురువుకు తెలియజేయండి మరియు అవసరమైతే క్లుప్తంగా దూరంగా ఉండండి.

ప్రశ్న 9: ఆన్‌లైన్ తరగతుల సమయంలో మీ టీచర్ నుండి స్పష్టత పొందడానికి సరైన మార్గం ఏమిటి?

ఎ) వారు గమనించినట్లు నిర్ధారించుకోవడానికి ఒకే ప్రశ్నతో బహుళ ఇమెయిల్‌లను పంపడం.

బి) సంభాషణను ప్రారంభించడానికి సంబంధం లేని ప్రశ్నలను అడగడం.

సి) నిర్దిష్ట మరియు సంబంధిత ప్రశ్నలను అడగడానికి చాట్ లేదా మెసేజింగ్ ఫీచర్‌ని ఉపయోగించడం.

డి) మీ అన్ని ప్రశ్నలను ఒకేసారి అడగడానికి తరగతి ముగిసే వరకు వేచి ఉండండి.

సమాధానం: సి) నిర్దిష్ట మరియు సంబంధిత ప్రశ్నలను అడగడానికి చాట్ లేదా మెసేజింగ్ ఫీచర్‌ని ఉపయోగించడం.

ప్రశ్న 10: మీరు ఆన్‌లైన్ క్లాస్ సెషన్‌ను ఎలా సరిగ్గా ముగించాలి?

ఎ) ఏమీ మాట్లాడకుండా అకస్మాత్తుగా క్లాస్ నుండి వెళ్ళిపోవడం.

బి) టీచర్‌కి కృతజ్ఞతలు తెలుపుతూ క్లాస్‌కి వెళ్లే ముందు వీడ్కోలు చెప్పడం.

సి) లాగ్ అవుట్ చేయకుండా అప్లికేషన్‌ను మూసివేయడం.

D) చాట్‌లో శీఘ్ర సందేశాన్ని పంపడం, ఆపై నిశ్శబ్దంగా నిష్క్రమించడం.

జవాబు: బి) టీచర్‌కి కృతజ్ఞతలు తెలుపుతూ, క్లాస్‌కి వెళ్లే ముందు వీడ్కోలు పలుకుతారు.

పబ్లిక్ కంప్యూటర్లు మరియు వైఫై:

ప్రశ్న 1: పబ్లిక్ కంప్యూటర్‌లు మరియు వైఫై నెట్‌వర్క్‌లు అంటే ఏమిటి?

ఎ) ప్రజల ఉపయోగం కోసం ప్రత్యేకంగా రూపొందించిన కంప్యూటర్లు.

బి) ప్రభుత్వం అందించిన కంప్యూటర్లు మరియు నెట్‌వర్క్‌లు.

సి) లైబ్రరీలు లేదా కేఫ్‌లు వంటి పబ్లిక్ ప్రదేశాలలో కంప్యూటర్‌లు మరియు నెట్‌వర్క్‌లు అందుబాటులో ఉన్నాయి.

డి) కంప్యూటర్లు మరియు నెట్‌వర్క్‌లు అధీకృత సిబ్బందికి మాత్రమే కేటాయించబడ్డాయి.

జవాబు: సి) లైబ్రరీలు లేదా కేఫ్‌లు వంటి పబ్లిక్ ప్రదేశాలలో ఉపయోగించడానికి కంప్యూటర్‌లు మరియు నెట్‌వర్క్‌లు అందుబాటులో ఉన్నాయి.

ప్రశ్న 2: పబ్లిక్ వైఫై నెట్‌వర్క్‌లను ఉపయోగిస్తున్నప్పుడు సంభావ్య భద్రతా ప్రమాదం ఏమిటి?

ఎ) ప్రైవేట్ నెట్‌వర్క్‌లతో పోలిస్తే వేగవంతమైన ఇంటర్నెట్ వేగం.

బి) నిర్దిష్ట వెబ్‌సైట్‌లకు యాక్సెస్ లేకపోవడం.

సి) డేటా అంతరాయం మరియు అనధికార యాక్సెస్ ప్రమాదం పెరిగింది.

D) మాల్వేర్ మరియు వైరస్ల నుండి రక్షణ హామీ.

సమాధానం: సి) డేటా అంతరాయం మరియు అనధికార యాక్సెస్ ప్రమాదం పెరిగింది.

ప్రశ్న 3: పబ్లిక్ కంప్యూటర్ లేదా వైఫై నెట్‌వర్క్‌ని ఉపయోగిస్తున్నప్పుడు మీరు ఏమి చేయకుండా ఉండాలి?

ఎ) మీ ఇమెయిల్ లేదా సోషల్ మీడియా ఖాతాలను యాక్సెస్ చేయడం.

బి) పెద్ద ఫైల్‌లు లేదా సాఫ్ట్‌వేర్ అప్‌డేట్‌లను డౌన్‌లోడ్ చేయడం.

సి) మీ బ్యాంక్ ఖాతాను తనిఖీ చేయడం లేదా ఆన్‌లైన్ కొనుగోళ్లు చేయడం.

డి) వైఫై పాస్‌వర్డ్‌ను సమీపంలోని ఇతరులతో పంచుకోవడం.

సమాధానం: సి) మీ బ్యాంక్ ఖాతాను తనిఖీ చేయడం లేదా ఆన్‌లైన్ కొనుగోళ్లు చేయడం.

ప్రశ్న 4: పబ్లిక్ వైఫైని ఉపయోగిస్తున్నప్పుడు మీరు మీ గోప్యత మరియు సున్నితమైన సమాచారాన్ని ఎలా రక్షించుకోవచ్చు?

ఎ) నెట్‌వర్క్ వేగాన్ని మెరుగుపరచడానికి మీ పరికరంలో ఫైర్‌వాల్‌ను నిలిపివేయండి.

బి) మీ ఇంటర్నెట్ కనెక్షన్‌ని గుప్తీకరించడానికి వర్చువల్ ప్రైవేట్ నెట్‌వర్క్ (VPN)ని ఉపయోగించండి.

సి) సమీపంలోని విశ్వసనీయ వ్యక్తులతో మాత్రమే మీ వ్యక్తిగత సమాచారాన్ని షేర్ చేయండి.

డి) పాస్‌వర్డ్‌ను మరచిపోకుండా ఉండటానికి మీ పరికరాన్ని అన్‌లాక్ చేసి ఉంచండి.

సమాధానం: బి) మీ ఇంటర్నెట్ కనెక్షన్‌ని గుప్తీకరించడానికి వర్చువల్ ప్రైవేట్ నెట్‌వర్క్ (VPN)ని ఉపయోగించండి.

ప్రశ్న 5: మీ ఖాతాల నుండి లాగ్ అవుట్ చేయడం మరియు పబ్లిక్ కంప్యూటర్‌లలో బ్రౌజింగ్ చరిత్రను క్లియర్ చేయడం ఎందుకు ముఖ్యం?

ఎ) మాల్వేర్ మరియు వైరస్ల నుండి రక్షించడానికి.

బి) కంప్యూటర్ పనితీరును మెరుగుపరచడం.

సి) తదుపరి వినియోగదారు మీ ఖాతాలు మరియు ప్రైవేట్ సమాచారాన్ని యాక్సెస్ చేయకుండా నిరోధించడానికి.

డి) కంప్యూటర్ నిల్వ సామర్థ్యాన్ని పెంచడానికి.

సమాధానం: సి) తదుపరి వినియోగదారు మీ ఖాతాలు మరియు ప్రైవేట్ సమాచారాన్ని యాక్సెస్ చేయకుండా నిరోధించడానికి.

ప్రశ్న 6: మీరు పబ్లిక్ కంప్యూటర్‌లో అనుమానాస్పద లేదా అనధికారిక కార్యకలాపాలను గమనించినట్లయితే మీరు ఏమి చేయాలి?

ఎ) దాన్ని విస్మరించండి మరియు కంప్యూటర్‌ను ఉపయోగించడం కొనసాగించండి.

బి) దానిని లైబ్రరీ లేదా కేఫ్ సిబ్బందికి నివేదించండి.

సి) కార్యకలాపాలకు బాధ్యత వహించే వ్యక్తిని ఎదుర్కోండి.

డి) సంఘటనను డాక్యుమెంట్ చేయడానికి ఫోటో లేదా వీడియో తీయండి.

సమాధానం: బి) దానిని లైబ్రరీ లేదా కేఫ్ సిబ్బందికి నివేదించండి.

ప్రశ్న 7: మీరు చట్టబద్ధమైన పబ్లిక్ వైఫై నెట్‌వర్క్‌ను ఎలా గుర్తించగలరు?

ఎ) దాని ప్రత్యేక నెట్‌వర్క్ పేరు (SSID) ద్వారా క్రమం తప్పకుండా మారుతుంది.

B) దాని సాధారణ మరియు సాధారణ నెట్‌వర్క్ పేరు (ఉదా., "FreeWiFi" లేదా "PublicWiFi") ద్వారా.

సి) నెట్‌వర్క్ పేరు పక్కన లాక్ గుర్తు ఉండటం ద్వారా.

D) సమీపంలోని అపరిచితులను వారు నెట్‌వర్క్‌ని గుర్తించారా అని అడగడం ద్వారా.

సమాధానం: సి) నెట్‌వర్క్ పేరు పక్కన లాక్ గుర్తు ఉండటం ద్వారా.

ప్రశ్న 8: వ్యక్తిగత ఖాతాలు లేదా సున్నితమైన డేటాను యాక్సెస్ చేయడానికి పబ్లిక్ కంప్యూటర్‌లను ఉపయోగించడం ఎందుకు సిఫార్సు చేయబడదు?

ఎ) పబ్లిక్ కంప్యూటర్‌లు అటువంటి పనుల కోసం వేగవంతమైన ప్రాసెసింగ్ వేగాన్ని కలిగి ఉంటాయి.

బి) పబ్లిక్ కంప్యూటర్లు మెరుగైన భద్రతా చర్యలను కలిగి ఉంటాయి.

సి) పబ్లిక్ కంప్యూటర్‌లలో కీలాగర్‌లు లేదా మాల్వేర్ ఇన్‌స్టాల్ చేయబడి ఉండవచ్చు.

D) పబ్లిక్ కంప్యూటర్లు ఉపయోగించిన తర్వాత మొత్తం బ్రౌజింగ్ చరిత్రను స్వయంచాలకంగా తొలగిస్తాయి.

జవాబు: సి) పబ్లిక్ కంప్యూటర్‌లలో కీలాగర్‌లు లేదా మాల్వేర్ ఇన్‌స్టాల్ చేయబడి ఉండవచ్చు.

ప్రశ్న 9: పబ్లిక్ కంప్యూటర్ల సందర్భంలో కీలాగర్ అంటే ఏమిటి?

ఎ) కంప్యూటర్‌ను అన్‌లాక్ చేయడానికి ఉపయోగించే పరికరం.

బి) టైపింగ్ వేగాన్ని పెంచడానికి ఉపయోగించే సాఫ్ట్‌వేర్.

సి) ఫైల్‌లను యాక్సెస్ చేయడానికి పాస్‌వర్డ్ అవసరమయ్యే సెక్యూరిటీ ఫీచర్.

D) సున్నితమైన సమాచారాన్ని క్యాప్చర్ చేయడానికి కీస్ట్రోక్‌లను రికార్డ్ చేసే హానికరమైన సాఫ్ట్‌వేర్.

సమాధానం: D) సున్నితమైన సమాచారాన్ని క్యాప్చర్ చేయడానికి కీస్ట్రోక్‌లను రికార్డ్ చేసే హానికరమైన సాఫ్ట్‌వేర్.

ప్రశ్న 10: పబ్లిక్ కంప్యూటర్ లేదా వైఫై నెట్‌వర్క్ నుండి నిష్క్రమించే ముందు మీరు ఏమి చేయాలి?

ఎ) మీ ఖాతాల నుండి లాగ్ అవుట్ చేయండి మరియు బ్రౌజింగ్ చరిత్రను క్లియర్ చేయండి.

బి) శక్తిని ఆదా చేయడానికి కంప్యూటర్‌ను అన్‌ప్లగ్ చేయండి.

సి) వైఫై నెట్‌వర్క్ పాస్‌వర్డ్‌ను మార్చండి.

D) కంప్యూటర్ పనితీరును మెరుగుపరచడానికి అదనపు సాఫ్ట్‌వేర్‌ను ఇన్‌స్టాల్ చేయండి.

సమాధానం: ఎ) మీ ఖాతాల నుండి లాగ్ అవుట్ చేయండి మరియు బ్రౌజింగ్ చరిత్రను క్లియర్ చేయండి.

**సురక్షిత డౌన్‌లోడ్‌లు:**

ప్రశ్న 1: "సురక్షిత డౌన్‌లోడ్‌లు" దేనిని సూచిస్తాయి?

ఎ) విశ్వసనీయ వెబ్‌సైట్‌ల నుండి మాత్రమే ఫైల్‌లను డౌన్‌లోడ్ చేయడం.

బి) హై-స్పీడ్ ఇంటర్నెట్ కనెక్షన్‌లను ఉపయోగించి ఫైల్‌లను డౌన్‌లోడ్ చేయడం.

సి) ఎటువంటి ధృవీకరణ ప్రక్రియ లేకుండా ఫైల్‌లను డౌన్‌లోడ్ చేయడం.

D) పరిమితులు లేకుండా ఏదైనా మూలం నుండి ఫైల్‌లను డౌన్‌లోడ్ చేయడం.

సమాధానం: ఎ) విశ్వసనీయ వెబ్‌సైట్‌ల నుండి మాత్రమే ఫైల్‌లను డౌన్‌లోడ్ చేయడం.

ప్రశ్న 2: సాఫ్ట్‌వేర్ మరియు అప్లికేషన్‌లను డౌన్‌లోడ్ చేయడానికి సురక్షితమైన మార్గాలలో ఒకటి ఏమిటి?

ఎ) అనేక డౌన్‌లోడ్ ఎంపికలతో అనధికారిక వెబ్‌సైట్‌ల నుండి డౌన్‌లోడ్ చేయడం.

బి) పీర్-టు-పీర్ ఫైల్-షేరింగ్ ప్లాట్‌ఫారమ్‌లను ఉపయోగించడం.

సి) అధికారిక వెబ్‌సైట్‌లు లేదా యాప్ స్టోర్‌ల నుండి డౌన్‌లోడ్ చేయడం.

D) ఇమెయిల్ లేదా సోషల్ మీడియా ద్వారా భాగస్వామ్యం చేయబడిన డౌన్‌లోడ్ లింక్‌లను ఉపయోగించడం.

సమాధానం: సి) అధికారిక వెబ్‌సైట్‌లు లేదా యాప్ స్టోర్‌ల నుండి డౌన్‌లోడ్ చేయడం.

ప్రశ్న 3: కొనసాగడానికి ముందు డౌన్‌లోడ్ మూలాన్ని ధృవీకరించడం ఎందుకు అవసరం?

ఎ) బ్యాండ్‌విడ్త్ వినియోగించే పెద్ద ఫైల్‌లను డౌన్‌లోడ్ చేయకుండా ఉండటానికి.

బి) ఫైల్ మీ పరికరానికి అనుకూలంగా ఉందని నిర్ధారించుకోవడానికి.

సి) మాల్వేర్ లేదా వైరస్‌లను డౌన్‌లోడ్ చేయకుండా రక్షించడానికి.

D) డౌన్‌లోడ్ ఉచితం లేదా చెల్లింపు అవసరమా అని తనిఖీ చేయడానికి.

సమాధానం: సి) మాల్వేర్ లేదా వైరస్‌లను డౌన్‌లోడ్ చేయకుండా రక్షించడానికి.

ప్రశ్న 4: సాఫ్ట్‌వేర్‌ను డౌన్‌లోడ్ చేయడానికి ముందు వినియోగదారు సమీక్షలను చదవడం యొక్క ఉద్దేశ్యం ఏమిటి?

ఎ) సాఫ్ట్‌వేర్ ధరను తెలుసుకోవడానికి.

బి) సాఫ్ట్‌వేర్ యొక్క ప్రజాదరణను నిర్ణయించడం.

సి) సాఫ్ట్‌వేర్ యొక్క లక్షణాలు మరియు కార్యాచరణ గురించి తెలుసుకోవడానికి.

D) సాఫ్ట్‌వేర్‌తో సంభావ్య సమస్యలు లేదా భద్రతా సమస్యలను కనుగొనడం.

సమాధానం: D) సాఫ్ట్‌వేర్‌తో సంభావ్య సమస్యలు లేదా భద్రతా సమస్యలను కనుగొనడానికి.

ప్రశ్న 5: మీరు తెలియని లేదా అవిశ్వసనీయ మూలాల ద్వారా పంపబడిన ఇమెయిల్ జోడింపుల నుండి ఫైల్‌లను డౌన్‌లోడ్ చేయడాన్ని ఎందుకు నివారించాలి?

ఎ) మీ పరికరంలో ఎక్కువ నిల్వ స్థలాన్ని తీసుకోకుండా ఉండటానికి.

బి) కాపీరైట్ చేయబడిన కంటెంట్‌ను డౌన్‌లోడ్ చేయకుండా రక్షించడానికి.

సి) మాల్వేర్ లేదా వైరస్‌లను డౌన్‌లోడ్ చేసే ప్రమాదాన్ని నివారించడానికి.

D) బహుళ డౌన్‌లోడ్ చేసిన ఫైల్‌లను నిర్వహించడంలో ఇబ్బందిని నివారించడానికి.

సమాధానం: సి) మాల్వేర్ లేదా వైరస్‌లను డౌన్‌లోడ్ చేసే ప్రమాదాన్ని నివారించడానికి.

ప్రశ్న 6: డౌన్‌లోడ్ చేసిన ఫైల్ తెరవడానికి ముందు సురక్షితంగా ఉందని మీరు ఎలా నిర్ధారించుకోవచ్చు?

ఎ) యాంటీవైరస్ ప్రోగ్రామ్‌ని ఉపయోగించి త్వరిత స్కాన్‌ను అమలు చేయండి.

బి) ఫైల్‌ని తనిఖీ చేయమని స్నేహితుడిని లేదా కుటుంబ సభ్యుడిని అడగండి.

సి) దాని భద్రతను గుర్తించడానికి ఫైల్ పరిమాణాన్ని తనిఖీ చేయండి.

D) ఫైల్‌ని తెరవడానికి ముందు గుర్తించదగిన పేరుకు పేరు మార్చండి.

సమాధానం: ఎ) యాంటీవైరస్ ప్రోగ్రామ్‌ని ఉపయోగించి త్వరిత స్కాన్‌ను అమలు చేయండి.

ప్రశ్న 7: డౌన్‌లోడ్ చేయబడిన ఫైల్ మీ యాంటీవైరస్ సాఫ్ట్‌వేర్ నుండి భద్రతా హెచ్చరికను ప్రేరేపిస్తే మీరు ఏమి చేయాలి?

ఎ) హెచ్చరికను విస్మరించి, ఫైల్‌ని తెరవడం కొనసాగించండి.

బి) ఫైల్‌ను తెరవడానికి యాంటీవైరస్ సాఫ్ట్‌వేర్‌ను తాత్కాలికంగా నిలిపివేయండి.

సి) ఫైల్‌ను వెంటనే క్వారంటైన్ చేయండి లేదా తొలగించండి.

D) సహాయం కోసం ఫైల్ సృష్టికర్తను సంప్రదించండి.

సమాధానం: సి) ఫైల్‌ను వెంటనే క్వారంటైన్ చేయండి లేదా తొలగించండి.

ప్రశ్న 8: మీ ఆపరేటింగ్ సిస్టమ్ మరియు యాంటీవైరస్ సాఫ్ట్‌వేర్‌ను తాజాగా ఉంచడం ఎందుకు కీలకం?

ఎ) సాఫ్ట్‌వేర్ యొక్క సౌందర్యం మరియు దృశ్యమాన ఆకర్షణను మెరుగుపరచడం.

బి) మీ కంప్యూటర్ ప్రాసెసింగ్ వేగాన్ని పెంచడానికి.

సి) కొత్త భద్రతా బెదిరింపులు మరియు దుర్బలత్వాల నుండి రక్షించడానికి.

D) సాఫ్ట్‌వేర్‌కు కొత్త ఫీచర్లు మరియు కార్యాచరణలను జోడించడానికి.

సమాధానం: సి) కొత్త భద్రతా బెదిరింపులు మరియు దుర్బలత్వాల నుండి రక్షించడానికి.

ప్రశ్న 9: డౌన్‌లోడ్ చేయడానికి ముందు ఫైల్ పొడిగింపును ధృవీకరించడం యొక్క ఉద్దేశ్యం ఏమిటి?

ఎ) ఫైల్ ఉచితం లేదా చెల్లింపు అవసరమా అని తనిఖీ చేయడానికి.

బి) ఫైల్ డౌన్‌లోడ్ వేగాన్ని నిర్ణయించడానికి.

సి) ఫైల్ మీ పరికరానికి అనుకూలంగా ఉందని నిర్ధారించుకోవడానికి.

D) ఫైల్ రకం మరియు దాని సంభావ్య ప్రమాదాలను గుర్తించడం.

సమాధానం: D) ఫైల్ రకం మరియు దాని సంభావ్య ప్రమాదాలను గుర్తించడానికి.

ప్రశ్న 10: అవాంఛిత ప్రోగ్రామ్‌లను (PUPలు) అనుకోకుండా డౌన్‌లోడ్ చేయడాన్ని మీరు ఎలా నివారించవచ్చు?

ఎ) ఇన్‌స్టాలేషన్ ప్రక్రియలో అన్ని నిబంధనలు మరియు షరతులను ఎల్లప్పుడూ అంగీకరించండి.

బి) వేగవంతమైన సెటప్ కోసం "ఎక్స్‌ప్రెస్" ఇన్‌స్టాలేషన్ ఎంపికను ఎంచుకోండి.

సి) "కస్టమ్" లేదా "అధునాతన" ఇన్‌స్టాలేషన్ ఎంపికను ఉపయోగించండి మరియు ప్రతి దశను జాగ్రత్తగా సమీక్షించండి.

D) ఎంపికలను పెంచడానికి వీలైనన్ని ఎక్కువ మూలాల నుండి ఫైల్‌లను డౌన్‌లోడ్ చేయండి.

సమాధానం: సి) "అనుకూల" లేదా "అధునాతన" ఇన్‌స్టాలేషన్ ఎంపికను ఉపయోగించండి మరియు ప్రతి దశను జాగ్రత్తగా సమీక్షించండి.

**మాల్వేర్ మరియు వైరస్**

ప్రశ్న 1:

మాల్వేర్ అంటే ఏమిటి?

ఎ) డేటా నిల్వ కోసం ఉపయోగించే హార్డ్‌వేర్ రకం

బి) వైరస్‌ల నుండి రక్షించడానికి రూపొందించబడిన సాఫ్ట్‌వేర్

సి) కంప్యూటర్ సిస్టమ్‌లకు హాని కలిగించే హానికరమైన సాఫ్ట్‌వేర్

D) నెట్‌వర్క్ ట్రాఫిక్‌ను నియంత్రించడానికి ఉపయోగించే సిస్టమ్

జవాబు: సి) కంప్యూటర్ సిస్టమ్‌లకు హాని కలిగించే హానికరమైన సాఫ్ట్‌వేర్

ప్రశ్న 2:

కింది వాటిలో ఏది మాల్వేర్ రకం కాదు?

ఎ) ట్రోజన్ హార్స్

బి) పురుగు

సి) ఫైర్‌వాల్

డి) Ransomware

సమాధానం: సి) ఫైర్‌వాల్

ప్రశ్న 3:

వైరస్ యొక్క ప్రధాన ప్రయోజనం ఏమిటి?

ఎ) కంప్యూటర్ పనితీరును మందగించడానికి

బి) కంప్యూటర్ నుండి ఫైళ్లను తొలగించడానికి

సి) ఇతర వ్యవస్థలకు ప్రతిరూపం మరియు వ్యాప్తి చెందడం

D) బాధించే పాప్-అప్ ప్రకటనలను ప్రదర్శించడానికి

జవాబు: సి) ఇతర వ్యవస్థలకు ప్రతిరూపం మరియు వ్యాప్తి చెందడం

ప్రశ్న 4:

మాల్వేర్ కంప్యూటర్ సిస్టమ్‌కు ఎలా సోకుతుంది?

ఎ) జోడింపులతో ఇమెయిల్ పంపడం ద్వారా

బి) ఆన్‌లైన్ గేమ్‌లు ఆడటం ద్వారా

సి) సురక్షితమైన మరియు నవీకరించబడిన ఆపరేటింగ్ సిస్టమ్‌ను ఉపయోగించడం ద్వారా

D) కంప్యూటర్ యొక్క యాంటీవైరస్ సాఫ్ట్‌వేర్‌ను ఆఫ్ చేయడం ద్వారా

సమాధానం: ఎ) జోడింపులతో ఇమెయిల్ పంపడం ద్వారా

ప్రశ్న 5:

రూట్‌కిట్ ఏమి చేస్తుంది?

ఎ) వైరస్‌ల నుండి కంప్యూటర్‌ను రక్షిస్తుంది

బి) కంప్యూటర్‌లోని ఫైల్‌లను ఎన్‌క్రిప్ట్ చేస్తుంది

సి) సిస్టమ్‌పై అనధికార యాక్సెస్ మరియు నియంత్రణను పొందుతుంది

D) డిస్క్ స్థలాన్ని ఖాళీ చేయడానికి తాత్కాలిక ఫైల్‌లను క్లియర్ చేస్తుంది

సమాధానం: సి) సిస్టమ్‌పై అనధికారిక యాక్సెస్ మరియు నియంత్రణను పొందుతుంది

ప్రశ్న 6:

కీలాగర్ అంటే ఏమిటి?

ఎ) ఒక రకమైన యాంటీవైరస్ సాఫ్ట్‌వేర్

బి) కంప్యూటర్ పనితీరును మెరుగుపరిచే హార్డ్‌వేర్ భాగం

సి) పాస్‌వర్డ్‌లు మరియు సున్నితమైన సమాచారంతో సహా కీస్ట్రోక్‌లను రికార్డ్ చేసే సాఫ్ట్‌వేర్

డి) USB డ్రైవ్‌ల ద్వారా వ్యాపించే వైరస్

జవాబు: సి) పాస్‌వర్డ్‌లు మరియు సున్నితమైన సమాచారంతో సహా కీస్ట్రోక్‌లను రికార్డ్ చేసే సాఫ్ట్‌వేర్

ప్రశ్న 7:

కింది వాటిలో మాల్వేర్ ఇన్ఫెక్షన్ యొక్క సాధారణ లక్షణం ఏది?

ఎ) వేగవంతమైన ఇంటర్నెట్ కనెక్షన్

బి) తగ్గిన CPU వినియోగం

సి) ఊహించని సిస్టమ్ క్రాష్ అవుతుంది లేదా ఫ్రీజ్ అవుతుంది

D) మెరుగైన కంప్యూటర్ పనితీరు

సమాధానం: సి) ఊహించని సిస్టమ్ క్రాష్ అవుతుంది లేదా ఫ్రీజ్ అవుతుంది

ప్రశ్న 8:

Ransomware యొక్క ప్రాథమిక లక్ష్యం ఏమిటి?

ఎ) వ్యక్తిగత సమాచారాన్ని దొంగిలించడానికి

బి) వినియోగదారుని వారి కంప్యూటర్ నుండి లాక్ చేయడం మరియు యాక్సెస్‌ని తిరిగి పొందడానికి చెల్లింపును డిమాండ్ చేయడం

సి) నెట్‌వర్క్ ట్రాఫిక్‌కు అంతరాయం కలిగించడానికి

D) దాని యొక్క కాపీలను సృష్టించడం మరియు ఇతర పరికరాలకు వ్యాప్తి చేయడం

సమాధానం: బి) వినియోగదారుని వారి కంప్యూటర్ నుండి లాక్ చేసి, యాక్సెస్‌ని తిరిగి పొందడానికి చెల్లింపును డిమాండ్ చేయడం

ప్రశ్న 9:

యాంటీవైరస్ సాఫ్ట్‌వేర్ ప్రయోజనం ఏమిటి?

A) కంప్యూటర్‌లో ఫైల్‌లు మరియు ఫోల్డర్‌లను గుప్తీకరించడానికి

బి) కంప్యూటర్ బూట్ సమయాన్ని వేగవంతం చేయడానికి

సి) మాల్వేర్ ఇన్ఫెక్షన్ల నుండి రక్షించడానికి మరియు తొలగించడానికి

డి) నిర్దిష్ట వెబ్‌సైట్‌లకు యాక్సెస్‌ను బ్లాక్ చేయడానికి

జవాబు: సి) మాల్వేర్ ఇన్ఫెక్షన్ల నుండి రక్షించడానికి మరియు తొలగించడానికి

ప్రశ్న 10:

మాల్‌వేర్ ఇన్‌ఫెక్షన్‌లను నివారించడంలో ఎలాంటి జాగ్రత్తలు సహాయపడతాయి?

ఎ) అనుమానాస్పద ఇమెయిల్ లింక్‌లు మరియు జోడింపులపై క్లిక్ చేయడం

బి) బలహీనమైన మరియు సులభంగా ఊహించగలిగే పాస్‌వర్డ్‌లను ఉపయోగించడం

సి) సాఫ్ట్‌వేర్‌ను ప్రసిద్ధ మూలాల నుండి మాత్రమే డౌన్‌లోడ్ చేయడం

డి) ఆటోమేటిక్ సాఫ్ట్‌వేర్ నవీకరణలను నిలిపివేయడం

సమాధానం: సి) సాఫ్ట్‌వేర్‌ను ప్రసిద్ధ మూలాల నుండి మాత్రమే డౌన్‌లోడ్ చేయడం

Day – 2

**ఆన్‌లైన్ గేమింగ్:**

ప్రశ్న 1:

మితిమీరిన ఆన్‌లైన్ గేమింగ్‌తో సంబంధం ఉన్న కొన్ని సంభావ్య శారీరక ఆరోగ్య హాని ఏమిటి?

ఎ) పెరిగిన సామాజిక పరస్పర చర్య

బి) మెరుగైన చేతి-కంటి సమన్వయం

సి) కంటి ఒత్తిడి, తలనొప్పులు మరియు పునరావృత ఒత్తిడి గాయాలు

డి) మెరుగైన కార్డియోవాస్కులర్ ఫిట్‌నెస్

సమాధానం: సి) కంటి ఒత్తిడి, తలనొప్పులు మరియు పునరావృత ఒత్తిడి గాయాలు

ప్రశ్న 2:

"గేమింగ్ అడిక్షన్" లేదా "ఇంటర్నెట్ గేమింగ్ డిజార్డర్" అంటే ఏమిటి?

ఎ) హింసాత్మక వీడియో గేమ్‌లకు గురికావడం వల్ల ఏర్పడే వైద్య పరిస్థితి

బి) ఒక వ్యక్తి అప్పుడప్పుడు ఆన్‌లైన్ గేమ్‌లు ఆడే పరిస్థితి, కానీ వ్యసనానికి గురికాదు

సి) రోజువారీ జీవితంలో జోక్యం చేసుకునే నిర్బంధ మరియు అధిక గేమింగ్ ప్రవర్తన

D) గేమ్‌ప్లే సమయంలో విసుగు యొక్క తాత్కాలిక స్థితి

జవాబు: సి) రోజువారీ జీవితంలో జోక్యం చేసుకునే నిర్బంధ మరియు అధిక గేమింగ్ ప్రవర్తన

ప్రశ్న 3:

విద్యావేత్తలు లేదా పనిపై అధిక ఆన్‌లైన్ గేమింగ్ యొక్క ప్రతికూల ప్రభావం క్రింది వాటిలో ఏది?

ఎ) మెరుగైన బహువిధి సామర్థ్యాలు

బి) మెరుగైన సమస్య పరిష్కార నైపుణ్యాలు

సి) తగ్గిన ఉత్పాదకత మరియు పేలవమైన విద్యా లేదా పని పనితీరు

డి) చదువులు లేదా వృత్తి జీవితంలో రాణించడానికి ప్రేరణ పెరిగింది

జవాబు: సి) ఉత్పాదకత తగ్గడం మరియు విద్యాపరమైన లేదా పని పనితీరు తక్కువగా ఉండటం

ప్రశ్న 4:

ఆన్‌లైన్ గేమింగ్‌తో సంబంధం ఉన్న కొన్ని సంభావ్య సామాజిక హాని ఏమిటి?

ఎ) సహచరులు మరియు పెద్దలతో కమ్యూనికేషన్ నైపుణ్యాలను మెరుగుపరచడం

బి) విభిన్న దృక్కోణాలపై సానుభూతి మరియు అవగాహన పెరగడం

సి) సామాజిక ఒంటరితనం మరియు నిజ జీవిత పరస్పర చర్యల నుండి ఉపసంహరణ

డి) కుటుంబం మరియు స్నేహితులతో సంబంధాలను బలోపేతం చేయడం

జవాబు: సి) సామాజిక ఒంటరితనం మరియు నిజ జీవిత పరస్పర చర్యల నుండి ఉపసంహరణ

ప్రశ్న 5:

ఆన్‌లైన్ గేమింగ్ సందర్భంలో "లూట్ బాక్స్‌లు" అంటే ఏమిటి మరియు అవి ఎందుకు హానికరం?

ఎ) ఆటలో స్థాయిని పెంచడం ద్వారా ఆటగాళ్ళు సంపాదించగల ప్రత్యేక సామర్థ్యాలు

B) ప్లేయర్‌లు కొనుగోలు చేయగల యాదృచ్ఛిక గేమ్‌లోని అంశాలను కలిగి ఉన్న వర్చువల్ బాక్స్‌లు

సి) ఆటలో కరెన్సీని నిల్వ చేయడానికి కంటైనర్లు

డి) ఆటగాళ్ళు శత్రువులకు వ్యతిరేకంగా జట్టుకట్టే సహకార గేమ్‌ప్లే మోడ్

సమాధానం: బి) ఆటగాళ్ళు కొనుగోలు చేయగల యాదృచ్ఛిక ఆటలోని వస్తువులను కలిగి ఉన్న వర్చువల్ బాక్స్‌లు

ప్రశ్న 6:

ఆన్‌లైన్ గేమింగ్ కమ్యూనిటీలలో సైబర్ బెదిరింపు ఎలా హాని కలిగించవచ్చు?

ఎ) ఆటగాళ్ళు ఆన్‌లైన్ ఫోరమ్‌లు మరియు చర్చలలో పాల్గొనవలసి ఉంటుంది

బి) ఆటలోని పాత్రలు ఒకదానితో ఒకటి విభేదాలు లేదా వైరుధ్యాలను కలిగి ఉండవచ్చు

సి) ఆటగాళ్ళు ఆటలో ఇతరులను అనామకంగా వేధించవచ్చు, భయపెట్టవచ్చు లేదా అవమానించవచ్చు

డి) ఆన్‌లైన్ గేమింగ్ సానుకూల సామాజిక పరస్పర చర్యలను మాత్రమే ప్రోత్సహిస్తుంది

జవాబు: సి) ఆటగాళ్ళు ఆటలో ఇతరులను అనామకంగా వేధించవచ్చు, భయపెట్టవచ్చు లేదా అవమానించవచ్చు

ప్రశ్న 7:

ఆన్‌లైన్ గేమింగ్ వ్యసనంతో సంబంధం ఉన్న కొన్ని సంభావ్య మానసిక హాని ఏమిటి?

ఎ) మెరుగైన ఆత్మగౌరవం మరియు ఆత్మవిశ్వాసం

బి) ఒత్తిడి మరియు ఆందోళన స్థాయిలను తగ్గించడం

సి) నిరాశ, ఆందోళన మరియు చిరాకు ప్రమాదం పెరుగుతుంది

D) మెరుగైన సమస్య-పరిష్కార నైపుణ్యాలు మరియు విమర్శనాత్మక ఆలోచన

సమాధానం: సి) నిరాశ, ఆందోళన మరియు చిరాకు ప్రమాదం పెరుగుతుంది

ప్రశ్న 8:

ఆన్‌లైన్ గేమింగ్‌లో నిమగ్నమైన యువకుల కోసం స్క్రీన్ సమయాన్ని పర్యవేక్షించడం మరియు నిర్వహించడం ఎందుకు అవసరం?

ఎ) ఆరోగ్యకరమైన శారీరక శ్రమ మరియు వ్యాయామాన్ని ప్రోత్సహించడం

బి) గేమింగ్ వ్యసనం మరియు దాని ప్రతికూల ప్రభావాలను నివారించడానికి

సి) అకడమిక్ లేదా పాఠ్యేతర కార్యకలాపాలకు ఎక్కువ సమయాన్ని అనుమతించడం

డి) కుటుంబ సభ్యులతో సామాజిక పరస్పర చర్యలను మెరుగుపరచడం

సమాధానం: బి) గేమింగ్ వ్యసనం మరియు దాని ప్రతికూల ప్రభావాలను నివారించడానికి

ప్రశ్న 9:

గేమ్‌లో కొనుగోళ్లు లేదా మైక్రోట్రాన్సాక్షన్‌లు ఆటగాళ్ళకు ఆర్థిక నష్టాలకు ఎలా దారితీస్తాయి?

ఎ) ఆటగాళ్ళు గేమ్‌ప్లే ద్వారా గేమ్‌లో కరెన్సీని సంపాదించవచ్చు

బి) గేమ్‌లో కొనుగోళ్లు ఊహించని విధంగా అధిక ఖర్చులకు దారితీయవచ్చు

సి) సూక్ష్మ లావాదేవీలు ఎల్లప్పుడూ సరసమైనవి మరియు ఎటువంటి ప్రమాదం లేదు

D) గేమ్‌లో కొనుగోళ్లు పూర్తిగా సౌందర్య సాధనాలు మరియు గేమ్‌ప్లేను ప్రభావితం చేయవు

సమాధానం: బి) గేమ్‌లో కొనుగోళ్లు ఊహించని విధంగా అధిక ఖర్చులకు దారితీయవచ్చు

ప్రశ్న 10:

ఆన్‌లైన్ గేమింగ్ సందర్భంలో "సైబర్‌ సెక్యూరిటీ రిస్క్" అంటే ఏమిటి?

ఎ) ఆటగాళ్ల వ్యక్తిగత సమాచారం దొంగిలించబడి దుర్వినియోగం అయ్యే ప్రమాదం

బి) గేమ్‌లోని పాత్రలు వర్చువల్ శత్రువులచే దాడి చేయబడే ప్రమాదం

సి) ఆటలో క్లిష్టమైన సవాళ్లను ఎదుర్కొనే ప్రమాదం

డి) గేమ్‌ప్లే సమయంలో ఇంటర్నెట్ కనెక్షన్ అంతరాయాల ప్రమాదం

జవాబు: ఎ) ఆటగాళ్ల వ్యక్తిగత సమాచారం దొంగిలించబడి దుర్వినియోగం అయ్యే ప్రమాదం

**సైబర్ వ్యసనం**

ప్రశ్న 1:

సైబర్ వ్యసనం లేదా ఇంటర్నెట్ వ్యసనం అంటే ఏమిటి?

ఎ) వ్యక్తులు కంప్యూటర్లు మరియు ఇంటర్నెట్‌ను ఉపయోగించడం పట్ల విరక్తి కలిగి ఉండే పరిస్థితి

బి) వ్యక్తులు అధికంగా మరియు నిర్బంధంగా ఇంటర్నెట్‌ను ఉపయోగించే ప్రవర్తన ప్రతికూల పరిణామాలకు దారితీస్తుంది

సి) సాంకేతికత మరియు ఆన్‌లైన్ కార్యకలాపాలతో సానుకూల మరియు ఆరోగ్యకరమైన నిశ్చితార్థం

D) సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లను అప్పుడప్పుడు ఉపయోగించడాన్ని వివరించడానికి ఉపయోగించే పదం

సమాధానం: బి) వ్యక్తులు ఇంటర్నెట్‌ను అధికంగా మరియు నిర్బంధంగా ఉపయోగించే ప్రవర్తన ప్రతికూల పరిణామాలకు దారితీస్తుంది

ప్రశ్న 2:

కింది వాటిలో సైబర్ వ్యసనం యొక్క సంభావ్య లక్షణం కానిది ఏది?

ఎ) వ్యక్తిగత బాధ్యతలు మరియు బాధ్యతలను విస్మరించడం

బి) ఆఫ్‌లైన్ కార్యకలాపాలు మరియు అభిరుచులపై ఆసక్తి కోల్పోవడం

సి) కుటుంబం మరియు స్నేహితులతో ఆరోగ్యకరమైన సంబంధాలను కొనసాగించడం

D) ఇంటర్నెట్‌ని ఉపయోగించనప్పుడు ఉపసంహరణ లక్షణాలను అనుభవించడం

జవాబు: సి) కుటుంబం మరియు స్నేహితులతో ఆరోగ్యకరమైన సంబంధాలను కొనసాగించడం

ప్రశ్న 3:

సైబర్ వ్యసనం వ్యక్తి యొక్క శారీరక ఆరోగ్యంపై ఎలా ప్రభావం చూపుతుంది?

ఎ) ఇది మెరుగైన ఫిట్‌నెస్ మరియు పెరిగిన శారీరక శ్రమకు దారితీస్తుంది

బి) ఇది నిద్ర భంగం మరియు ఇతర ఆరోగ్య సమస్యలను కలిగిస్తుంది

సి) ఇది చేతి-కంటి సమన్వయం మరియు మోటార్ నైపుణ్యాలను పెంచుతుంది

డి) ఇది భంగిమను మెరుగుపరుస్తుంది మరియు పునరావృతమయ్యే స్ట్రెయిన్ గాయాల ప్రమాదాన్ని తగ్గిస్తుంది

సమాధానం: బి) ఇది నిద్ర భంగం మరియు ఇతర ఆరోగ్య సమస్యలను కలిగిస్తుంది

ప్రశ్న 4:

సైబర్ వ్యసనానికి సంబంధించిన "ఫబ్బింగ్" అంటే ఏమిటి?

ఎ) ఆన్‌లైన్ ఈవెంట్‌లను కోల్పోతారనే భయాన్ని వివరించడానికి ఉపయోగించే పదం

బి) ఒకరి ఫోన్ లేదా ఇతర డిజిటల్ పరికరాలపై దృష్టి సారించడం ద్వారా నిజ జీవిత సంభాషణలు లేదా పరస్పర చర్యలను విస్మరించడం

సి) వ్యక్తిగత డేటాకు అనధికారిక యాక్సెస్ పొందడానికి హ్యాకర్లు ఉపయోగించే టెక్నిక్

డి) ఒక రకమైన ఆన్‌లైన్ గేమ్ వ్యసనం

సమాధానం: బి) ఒకరి ఫోన్ లేదా ఇతర డిజిటల్ పరికరాలపై దృష్టి సారించడం ద్వారా నిజ జీవిత సంభాషణలు లేదా పరస్పర చర్యలను విస్మరించడం

ప్రశ్న 5:

సైబర్ వ్యసనంతో సంబంధం ఉన్న కొన్ని సంభావ్య సామాజిక హాని ఏమిటి?

ఎ) మెరుగైన కమ్యూనికేషన్ నైపుణ్యాలు మరియు భావోద్వేగ మేధస్సు

బి) ఆన్‌లైన్ పరస్పర చర్యల ద్వారా కుటుంబ బంధాలను బలోపేతం చేయడం

సి) ముఖాముఖి సామాజిక పరస్పర చర్యలు మరియు ఒంటరితనం తగ్గింది

డి) సంబంధాలలో వైరుధ్యాలను నిర్వహించే మెరుగైన సామర్థ్యం

జవాబు: సి) ముఖాముఖి సామాజిక పరస్పర చర్యలు మరియు ఒంటరితనం తగ్గింది

ప్రశ్న 6:

సైబర్ వ్యసనం విద్యా లేదా పని పనితీరును ఎలా ప్రభావితం చేస్తుంది?

ఎ) ఇది ఏకాగ్రత మరియు ఉత్పాదకతను మెరుగుపరచడానికి దారితీస్తుంది

బి) ఇది మెరుగైన సమయ నిర్వహణ నైపుణ్యాలకు దారితీయవచ్చు

సి) ఇది ఫోకస్ తగ్గడం, తక్కువ గ్రేడ్‌లు మరియు తగ్గిన పని పనితీరుకు కారణమవుతుంది

డి) ఇది అకడమిక్ లేదా పని సంబంధిత పనులపై ఆసక్తిని పెంచుతుంది

సమాధానం: సి) ఇది దృష్టిని తగ్గించడం, తక్కువ గ్రేడ్‌లు మరియు పని పనితీరు తగ్గడం వంటి వాటికి కారణమవుతుంది

ప్రశ్న 7:

సైబర్ వ్యసనంతో సంబంధం ఉన్న కొన్ని సంభావ్య మానసిక హాని ఏమిటి?

ఎ) మెరుగైన మానసిక స్థితిస్థాపకత మరియు కోపింగ్ మెకానిజమ్స్

బి) ఒత్తిడి మరియు ఆందోళన స్థాయిలను తగ్గించడం

సి) డిప్రెషన్, ఒంటరితనం మరియు మూడ్ స్వింగ్‌ల ప్రమాదం పెరుగుతుంది

D) సైబర్ బెదిరింపును నిర్వహించే మెరుగైన సామర్థ్యం

జవాబు: సి) డిప్రెషన్, ఒంటరితనం మరియు మూడ్ స్వింగ్‌ల ప్రమాదం పెరుగుతుంది

ప్రశ్న 8:

సైబర్ వ్యసనం సందర్భంలో "డిజిటల్ హోర్డింగ్" అంటే ఏమిటి?

ఎ) డిజిటల్ టెక్నాలజీకి సంబంధించిన భౌతిక వస్తువులను వ్యక్తులు అధికంగా సేకరించే పరిస్థితి

బి) అధిక డిజిటల్ ఫైల్‌లు లేదా డేటాను ఆర్గనైజ్ చేయకుండా లేదా ఉపయోగించకుండా వాటిని పొందడం మరియు సేకరించడం అలవాటు

సి) వ్యక్తులు ఆన్‌లైన్‌లో ఇతరులను వేధించే సైబర్ బెదిరింపు యొక్క ఒక రూపం

డి) డిజిటల్ వస్తువులు మరియు సేవల కోసం షాపింగ్ చేసే వ్యసనం

జవాబు: బి) అధిక డిజిటల్ ఫైల్‌లు లేదా డేటాను ఆర్గనైజ్ చేయకుండా లేదా ఉపయోగించకుండా వాటిని సంపాదించడం మరియు సేకరించడం అలవాటు

ప్రశ్న 9:

సైబర్ వ్యసనాన్ని గుర్తించడం మరియు పరిష్కరించడం ఎందుకు కీలకం?

ఎ) ఎందుకంటే సైబర్ వ్యసనం తీవ్రమైన ఆందోళన కాదు మరియు ఎటువంటి ముఖ్యమైన సమస్యలకు దారితీయదు

బి) వ్యక్తులు ఆధునిక సాంకేతికత మరియు డిజిటల్ ప్రపంచంతో నిమగ్నమై ఉండేలా చేయడం

సి) శారీరక, మానసిక మరియు సామాజిక శ్రేయస్సుపై సంభావ్య ప్రతికూల పరిణామాలను నివారించడానికి

D) ఆఫ్‌లైన్ కార్యకలాపాలను మాత్రమే స్వీకరించమని వ్యక్తులను ప్రోత్సహించడం

సమాధానం: సి) శారీరక, మానసిక మరియు సామాజిక శ్రేయస్సుపై సంభావ్య ప్రతికూల పరిణామాలను నివారించడానికి

ప్రశ్న 10:

సైబర్ వ్యసనాన్ని నిర్వహించడంలో తల్లిదండ్రులు లేదా సంరక్షకులు తమ పిల్లలకు ఎలా మద్దతు ఇవ్వగలరు?

ఎ) స్వాతంత్య్రాన్ని పెంపొందించడానికి అపరిమిత ఇంటర్నెట్ యాక్సెస్‌ను ప్రోత్సహించడం ద్వారా

బి) పిల్లలను వినోదభరితంగా ఉంచడానికి బహుళ డిజిటల్ పరికరాలకు ప్రాప్యతను అందించడం ద్వారా

సి) సరిహద్దులను సెట్ చేయడం, స్క్రీన్ సమయాన్ని పర్యవేక్షించడం మరియు ఆన్‌లైన్ మరియు ఆఫ్‌లైన్ కార్యకలాపాల మధ్య ఆరోగ్యకరమైన బ్యాలెన్స్‌ను ప్రోత్సహించడం ద్వారా

డి) ఆన్‌లైన్ భద్రత మరియు గోప్యత గురించి చర్చలను నివారించడం ద్వారా

సమాధానం: సి) సరిహద్దులను సెట్ చేయడం, స్క్రీన్ సమయాన్ని పర్యవేక్షించడం మరియు ఆన్‌లైన్ మరియు ఆఫ్‌లైన్ కార్యకలాపాల మధ్య ఆరోగ్యకరమైన సమతుల్యతను ప్రోత్సహించడం ద్వారా

**ఆన్‌లైన్ ప్రెడేటర్‌లు మరియు పిల్లల ఆన్‌లైన్ కార్యాచరణ రక్షణ**

ప్రశ్న 1:

ఆన్‌లైన్ ప్రెడేటర్స్ ఎవరు?

ఎ) చట్టపరమైన మరియు నైతికమైన ఆన్‌లైన్ కార్యకలాపాలలో పాల్గొనే వ్యక్తులు

బి) ఇంటర్నెట్ మరియు సోషల్ మీడియాను ఎక్కువగా ఉపయోగించే వ్యక్తులు

సి) పిల్లలను దోపిడీ చేయడానికి మరియు హాని చేయడానికి ఇంటర్నెట్‌ను ఉపయోగించే వ్యక్తులు

డి) పోటీ మల్టీప్లేయర్ గేమ్‌లను ఆడే ఆన్‌లైన్ గేమర్‌లు

జవాబు: సి) పిల్లలను దోపిడీ చేయడానికి మరియు హాని చేయడానికి ఇంటర్నెట్‌ను ఉపయోగించే వ్యక్తులు

ప్రశ్న 2:

ఆన్‌లైన్ ప్రెడేటర్‌లు ఆన్‌లైన్‌లో పిల్లలను సంప్రదించడానికి ప్రయత్నించే ఒక మార్గం ఏమిటి?

ఎ) ప్రోత్సాహకరమైన మరియు సహాయక సందేశాలను పంపడం

బి) విద్యా మరియు సమాచార కంటెంట్‌ను పంచుకోవడం

సి) పిల్లలపై నమ్మకాన్ని పొందడానికి మరియు తారుమారు చేయడానికి మోసపూరిత వ్యూహాలను ఉపయోగించడం

D) పాఠశాల ప్రాజెక్ట్‌లో సహాయం కోసం అడగడం

జవాబు: సి) పిల్లలపై నమ్మకాన్ని పొందడానికి మరియు తారుమారు చేయడానికి మోసపూరిత వ్యూహాలను ఉపయోగించడం

ప్రశ్న 3:

ఆన్‌లైన్ భద్రత గురించి పిల్లలకు అవగాహన కల్పించడం ఎందుకు కీలకం?

ఎ) పిల్లలు ఇంటర్నెట్ మరియు సోషల్ మీడియాను ఉపయోగించకుండా నిరుత్సాహపరచడం

బి) సంభావ్య ప్రమాదాలను గుర్తించడానికి మరియు ఆన్‌లైన్‌లో తమను తాము రక్షించుకోవడానికి పిల్లలను శక్తివంతం చేయడం

సి) అధిక స్క్రీన్ సమయం మరియు ఆన్‌లైన్ ఎంగేజ్‌మెంట్‌ను ప్రోత్సహించడానికి

D) పిల్లలను ఆన్‌లైన్ ప్రెడేటర్‌లకు మరింత హాని కలిగించేలా చేయడం

జవాబు: బి) సంభావ్య ప్రమాదాలను గుర్తించి, ఆన్‌లైన్‌లో తమను తాము రక్షించుకునేలా పిల్లలను శక్తివంతం చేయడం

ప్రశ్న 4:

ఆన్‌లైన్ ప్రెడేటర్‌ల సందర్భంలో "గ్రూమింగ్" అంటే ఏమిటి?

ఎ) పిల్లల ఆన్‌లైన్ లెర్నింగ్ ప్రోగ్రామ్‌లను వివరించడానికి ఉపయోగించే పదం

బి) ఆన్‌లైన్ ప్రెడేటర్‌లు పిల్లలను తర్వాత దోపిడీ చేయడానికి వారితో నమ్మకాన్ని పెంచుకునే ప్రక్రియ

సి) ఆరోగ్యకరమైన ఆన్‌లైన్ పరస్పర చర్యలను ప్రోత్సహించే వ్యూహం

డి) పిల్లలు వీడియో గేమ్‌లు ఆడేందుకు ఎక్కువ సమయం కేటాయించేలా ప్రోత్సహించే టెక్నిక్

సమాధానం: బి) ఆన్‌లైన్ ప్రెడేటర్‌లు పిల్లలను తర్వాత దోపిడీ చేయడానికి వారితో నమ్మకాన్ని పెంచుకునే ప్రక్రియ

ప్రశ్న 6:

వారు ఆన్‌లైన్‌లో అనుమానాస్పద లేదా అసౌకర్య ప్రవర్తనను ఎదుర్కొంటే ఏమి చేయాలి?

ఎ) వ్యక్తిని నిరోధించండి మరియు ప్రవర్తనను విస్మరించండి

బి) వ్యక్తిని ఎదుర్కొని వారిని ఆపమని అడగండి

సి) నమ్మకాన్ని స్థాపించడానికి వ్యక్తిగత సమాచారాన్ని పంచుకోండి

డి) వెంటనే పరిస్థితి గురించి విశ్వసనీయ పెద్దలకు చెప్పండి

సమాధానం: డి) వెంటనే పరిస్థితి గురించి విశ్వసనీయ పెద్దలకు చెప్పండి

ప్రశ్న 7:

పిల్లలు తమ వ్యక్తిగత సమాచారాన్ని ఆన్‌లైన్‌లో గోప్యంగా ఉంచడం ఎందుకు అవసరం?

ఎ) స్నేహితులను ఆకట్టుకోవడానికి మరియు ఆన్‌లైన్ కమ్యూనిటీలలో ప్రజాదరణ పొందేందుకు

బి) ఆన్‌లైన్‌లో అపరిచితులతో బలమైన కనెక్షన్‌లను నిర్మించడం

సి) సంభావ్య ఆన్‌లైన్ ప్రమాదాలు మరియు గుర్తింపు దొంగతనం నుండి తమను తాము రక్షించుకోవడానికి

D) ప్రత్యేకమైన ఆన్‌లైన్ కంటెంట్ మరియు సేవలను యాక్సెస్ చేయడానికి

సమాధానం: సి) సంభావ్య ఆన్‌లైన్ ప్రమాదాలు మరియు గుర్తింపు దొంగతనం నుండి తమను తాము రక్షించుకోవడానికి

**సైబర్ స్టాకింగ్**

ప్రశ్న 1:

సైబర్‌స్టాకింగ్ అంటే ఏమిటి?

ఎ) ఆన్‌లైన్ గేమింగ్ వ్యసనం యొక్క ఒక రూపం

బి) బహుళ గ్రహీతలకు స్పామ్ ఇమెయిల్‌లను పంపే పద్ధతి

సి) నిరంతర మరియు అవాంఛిత ఆన్‌లైన్ వేధింపులు మరియు బెదిరింపుల నమూనా

D) వ్యక్తిగత సమాచారాన్ని ఆన్‌లైన్‌లో రక్షించడానికి ఉపయోగించే సాంకేతికత

సమాధానం: సి) నిరంతర మరియు అవాంఛిత ఆన్‌లైన్ వేధింపులు మరియు బెదిరింపుల నమూనా

ప్రశ్న 2:

సైబర్‌స్టాకింగ్ కోసం సాధారణంగా ఏ ఆన్‌లైన్ ప్లాట్‌ఫారమ్‌లు ఉపయోగించబడతాయి?

ఎ) ఆన్‌లైన్ బ్యాంకింగ్ వెబ్‌సైట్‌లు

బి) సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లు, మెసేజింగ్ యాప్‌లు మరియు ఇమెయిల్

సి) విద్యా వెబ్‌సైట్‌లు మరియు అభ్యాస వేదికలు

డి) షాపింగ్ కోసం ఇ-కామర్స్ వెబ్‌సైట్‌లు

సమాధానం: బి) సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లు, మెసేజింగ్ యాప్‌లు మరియు ఇమెయిల్

ప్రశ్న 3:

సైబర్‌స్టాకింగ్ ప్రవర్తన వెనుక కొన్ని సంభావ్య ప్రేరణలు ఏమిటి?

ఎ) బాధితుడి శ్రేయస్సు పట్ల నిజమైన శ్రద్ధ

బి) బాధితుడితో సానుకూల సంబంధాలను ఏర్పరచుకోవడం

సి) పగ, ముట్టడి లేదా బాధితుడిపై నియంత్రణ కోసం కోరిక

డి) విసుగు మరియు ఇతర ఆన్‌లైన్ కార్యకలాపాలు లేకపోవడం

సమాధానం: సి) ప్రతీకారం, ముట్టడి లేదా బాధితుడిపై నియంత్రణ కోసం కోరిక

ప్రశ్న 4:

సైబర్‌స్టాకింగ్ బాధితుడి మానసిక ఆరోగ్యాన్ని ఎలా ప్రతికూలంగా ప్రభావితం చేస్తుంది?

ఎ) బాధితుడి ఆత్మవిశ్వాసం మరియు ఆత్మగౌరవాన్ని మెరుగుపరచడం ద్వారా

బి) ఆన్‌లైన్‌లో సానుకూల సామాజిక పరస్పర చర్యలను ప్రోత్సహించడం ద్వారా

సి) భయం, ఆందోళన, నిరాశ మరియు మానసిక క్షోభ కలిగించడం ద్వారా

డి) బాధితుని ప్రజాదరణ మరియు సామాజిక స్థితిని పెంచడం ద్వారా

జవాబు: సి) భయం, ఆందోళన, నిరాశ మరియు మానసిక క్షోభ కలిగించడం ద్వారా

ప్రశ్న 5:

ఎవరైనా సైబర్‌స్టాకింగ్‌కు గురయ్యే అవకాశం ఉన్న కొన్ని సంభావ్య హెచ్చరిక సంకేతాలు ఏమిటి?

ఎ) సోషల్ మీడియాలో వ్యక్తిగత సమాచారాన్ని బహిరంగంగా పంచుకోవడం

బి) ఆన్‌లైన్ పరస్పర చర్యలపై అధికారం మరియు నియంత్రణలో ఉన్న అనుభూతి

సి) అపరిచితుల నుండి అధిక అభినందనలు మరియు సానుకూల సందేశాలను స్వీకరించడం

D) పదేపదే అవాంఛిత సందేశాలు, బెదిరింపులు లేదా వెంబడించే ప్రవర్తనలను స్వీకరించడం

సమాధానం: D) పదేపదే అవాంఛిత సందేశాలు, బెదిరింపులు లేదా వెంబడించే ప్రవర్తనలను స్వీకరించడం

ప్రశ్న 6:

వ్యక్తులు సైబర్‌స్టాకింగ్ నుండి తమను తాము ఎలా రక్షించుకోవచ్చు?

ఎ) ఆన్‌లైన్‌లో ఇతరులతో నమ్మకాన్ని పెంచుకోవడానికి వ్యక్తిగత సమాచారాన్ని ఉచితంగా పంచుకోవడం ద్వారా

బి) అపరిచితులతో తరచుగా ఆన్‌లైన్ వాదనలలో పాల్గొనడం ద్వారా

సి) సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లలో బలమైన గోప్యతా సెట్టింగ్‌లను సెట్ చేయడం ద్వారా

డి) ఆన్‌లైన్‌లో వారి లొకేషన్ మరియు రోజువారీ దినచర్యలను బహిరంగంగా బహిర్గతం చేయడం ద్వారా

సమాధానం: సి) సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లలో బలమైన గోప్యతా సెట్టింగ్‌లను సెట్ చేయడం ద్వారా

ప్రశ్న 7:

సైబర్‌స్టాకింగ్ బాధితులు తమను తాము రక్షించుకోవడానికి మరియు సహాయం కోసం ఏమి చేయాలి?

ఎ) సైబర్‌స్టాకర్ సందేశాలు మరియు డిమాండ్‌లకు ప్రతిస్పందించండి

బి) సైబర్‌స్టాకింగ్ సంఘటనలను రహస్యంగా ఉంచండి మరియు ఎవరికీ చెప్పకుండా ఉండండి

సి) సైబర్‌స్టాకింగ్‌కు సంబంధించిన డాక్యుమెంట్ సాక్ష్యం మరియు దానిని తగిన అధికారులకు లేదా ప్లాట్‌ఫారమ్ నిర్వాహకులకు నివేదించండి

డి) సైబర్‌స్టాకర్‌ను వ్యక్తిగతంగా ఎదుర్కొనే ప్రయత్నం

జవాబు: సి) సైబర్‌స్టాకింగ్‌కు సంబంధించిన డాక్యుమెంట్ సాక్ష్యం మరియు దానిని సంబంధిత అధికారులు లేదా ప్లాట్‌ఫారమ్ నిర్వాహకులకు నివేదించండి

ప్రశ్న 8:

సైబర్‌స్టాకింగ్ కోసం సాంకేతికతను ఒక సాధనంగా ఎలా దుర్వినియోగం చేయవచ్చు?

ఎ) ఆన్‌లైన్ ప్లాట్‌ఫారమ్‌లను బాధ్యతాయుతంగా మరియు గౌరవప్రదంగా ఉపయోగించడం ద్వారా

బి) స్నేహితులు మరియు అనుచరులతో సానుకూల మరియు ఉత్తేజకరమైన కంటెంట్‌ను పంచుకోవడం ద్వారా

సి) ఒకరి ఆన్‌లైన్ కార్యకలాపాన్ని వారి అనుమతి లేకుండా ట్రాక్ చేయడం ద్వారా

D) సహకార ఆన్‌లైన్ ప్రాజెక్ట్‌లు మరియు టీమ్‌వర్క్‌లో పాల్గొనడం ద్వారా

సమాధానం: సి) వారి అనుమతి లేకుండా వారి ఆన్‌లైన్ కార్యాచరణను ట్రాక్ చేయడం ద్వారా

ప్రశ్న 9:

అనేక అధికార పరిధిలో సైబర్‌స్టాకింగ్ యొక్క చట్టపరమైన పరిణామాలు ఏమిటి?

ఎ) సైబర్‌స్టాకింగ్ నేరంగా పరిగణించబడనందున ఎటువంటి చట్టపరమైన పరిణామాలు లేవు

బి) హెచ్చరికలు లేదా తాత్కాలిక ఖాతా సస్పెన్షన్‌లు వంటి స్వల్ప జరిమానాలు

సి) జరిమానాలు మరియు జైలు శిక్షతో సహా తీవ్రమైన జరిమానాలు

డి) బాధితుడు మరియు సైబర్‌స్టాకర్ ఇద్దరికీ కమ్యూనిటీ సేవ

సమాధానం: సి) జరిమానాలు మరియు జైలు శిక్షతో సహా తీవ్రమైన జరిమానాలు

ప్రశ్న 10:

సైబర్‌స్టాకింగ్‌ను నిరోధించడంలో ప్రేక్షకులు ఎలాంటి పాత్ర పోషిస్తారు?

ఎ) వారు సైబర్‌స్టాకింగ్ సంఘటనలను విస్మరించవచ్చు మరియు జోక్యం చేసుకోలేరు

బి) వారు వినోదం కోసం వారి కార్యకలాపాలలో సైబర్‌స్టాకర్‌తో చేరవచ్చు

సి) వారు బాధితుడికి మద్దతు ఇవ్వగలరు మరియు సైబర్‌స్టాకింగ్ ప్రవర్తనను అధికారులకు నివేదించవచ్చు

డి) వారు నేరుగా సైబర్‌స్టాకర్‌ను ఎదుర్కోవడానికి బాధితుడిని ప్రోత్సహించగలరు

సమాధానం: సి) వారు బాధితుడికి మద్దతు ఇవ్వగలరు మరియు సైబర్‌స్టాకింగ్ ప్రవర్తనను అధికారులకు నివేదించవచ్చు

**ఆన్‌లైన్ వేషధారణ:**

ప్రశ్న 1:

ఆన్‌లైన్ గ్రూమింగ్ అంటే ఏమిటి?

ఎ) ఆన్‌లైన్‌లో ఆరోగ్యకరమైన మరియు సానుకూల సంబంధాలను నిర్మించే ప్రక్రియ

బి) ఇంటర్నెట్‌లో వ్యక్తిగత సమాచారాన్ని రక్షించే సాంకేతికత

సి) ఆన్‌లైన్ వేధింపు మరియు బెదిరింపు యొక్క ఒక రూపం

D) లైంగిక ప్రయోజనాల కోసం పిల్లలను తారుమారు చేయడం మరియు దోపిడీ చేయడం

జవాబు: D) లైంగిక ప్రయోజనాల కోసం పిల్లలను తారుమారు చేయడం మరియు దోపిడీ చేయడం

ప్రశ్న 2:

ఆన్‌లైన్ వేషధారణ యొక్క సాధారణ లక్ష్యాలు ఎవరు?

ఎ) ఆన్‌లైన్ డేటింగ్‌లో పాల్గొనే పెద్దలు

బి) పిల్లలు మరియు యువకులు

సి) చట్ట అమలు అధికారులు ఆన్‌లైన్ కార్యకలాపాలను పర్యవేక్షిస్తారు

D) తల్లిదండ్రులు మరియు సంరక్షకులు తమ పిల్లల ఆన్‌లైన్ భద్రత గురించి ఆందోళన చెందుతున్నారు

సమాధానం: బి) పిల్లలు మరియు యువకులు

ప్రశ్న 3:

ఆన్‌లైన్ గ్రూమర్‌లు సాధారణంగా పిల్లల నమ్మకాన్ని ఎలా పొందుతారు?

ఎ) వారి నిజమైన గుర్తింపు మరియు ఉద్దేశాలను బహిరంగంగా బహిర్గతం చేయడం ద్వారా

బి) పిల్లవాడికి తెలిసిన లేదా విశ్వసించగల వ్యక్తిగా నటించడం ద్వారా

సి) వ్యక్తిగత సమాచారాన్ని పంచుకోకుండా పిల్లలను నిరుత్సాహపరచడం ద్వారా

D) సానుకూల మరియు ఆరోగ్యకరమైన ఆన్‌లైన్ పరస్పర చర్యలను ప్రోత్సహించడం ద్వారా

సమాధానం: బి) పిల్లవాడికి తెలిసిన లేదా విశ్వసించగల వ్యక్తిగా నటించడం ద్వారా

ప్రశ్న 5:

పిల్లలు ఆన్‌లైన్ వేషధారణకు బాధితురాలిగా ఉండే కొన్ని సంభావ్య సంకేతాలు ఏమిటి?

ఎ) పాఠశాల మరియు పాఠ్యేతర కార్యకలాపాలపై ఆసక్తిని పెంచడం

బి) ఆన్‌లైన్ పరస్పర చర్యల గురించి కుటుంబం మరియు స్నేహితులతో తరచుగా కమ్యూనికేట్ చేయడం

సి) కుటుంబం మరియు ఆఫ్‌లైన్ స్నేహితుల నుండి ఆకస్మిక ఉపసంహరణ

డి) ఆన్‌లైన్‌లో వ్యక్తిగత సమాచారాన్ని బహిరంగంగా పంచుకోవడం

సమాధానం: సి) కుటుంబం మరియు ఆఫ్‌లైన్ స్నేహితుల నుండి ఆకస్మిక ఉపసంహరణ

ప్రశ్న 6:

ఆన్‌లైన్ వస్త్రధారణ జరిగే కొన్ని ఆన్‌లైన్ ప్లాట్‌ఫారమ్‌లు ఏమిటి?

ఎ) పిల్లల బొమ్మలు మరియు దుస్తుల కోసం షాపింగ్ వెబ్‌సైట్‌లు

బి) విద్యా వెబ్‌సైట్‌లు మరియు అభ్యాస వేదికలు

సి) సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లు, మెసేజింగ్ యాప్‌లు మరియు ఆన్‌లైన్ గేమింగ్ కమ్యూనిటీలు

డి) ప్రభుత్వ వెబ్‌సైట్‌లు మరియు అధికారిక పోర్టల్‌లు

సమాధానం: సి) సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లు, మెసేజింగ్ యాప్‌లు మరియు ఆన్‌లైన్ గేమింగ్ కమ్యూనిటీలు

ప్రశ్న 7:

ఆన్‌లైన్ వస్త్రధారణను నిరోధించడంలో తల్లిదండ్రులు మరియు సంరక్షకులు ఏ పాత్ర పోషిస్తారు?

ఎ) వారి పిల్లల ఆన్‌లైన్ కార్యకలాపాలను విస్మరించడం మరియు వారి తీర్పును విశ్వసించడం

బి) ఆన్‌లైన్ ప్రమాదాలు మరియు భద్రత గురించి బహిరంగ మరియు నిజాయితీతో కూడిన సంభాషణలు కలిగి ఉండటం

సి) పిల్లలను రక్షించడానికి అన్ని ఇంటర్నెట్ మరియు సోషల్ మీడియా వినియోగాన్ని పరిమితం చేయడం

D) నమ్మకాన్ని పెంపొందించడానికి వ్యక్తిగత సమాచారాన్ని ఆన్‌లైన్‌లో పంచుకునేలా పిల్లలను ప్రోత్సహించడం

సమాధానం: బి) ఆన్‌లైన్ ప్రమాదాలు మరియు భద్రత గురించి బహిరంగ మరియు నిజాయితీ సంభాషణలు కలిగి ఉండటం

ప్రశ్న 8:

పిల్లల బాధితులపై ఆన్‌లైన్ వస్త్రధారణ వల్ల కలిగే కొన్ని మానసిక ప్రభావాలు ఏమిటి?

ఎ) పెరిగిన ఆత్మగౌరవం మరియు విశ్వాసం

బి) పెరిగిన సామాజిక పరస్పర చర్యలు మరియు సానుకూల సంబంధాలు

సి) భావోద్వేగ బాధ, భయం మరియు ఆందోళన

D) మెరుగైన విద్యా పనితీరు మరియు దృష్టి

సమాధానం: సి) భావోద్వేగ బాధ, భయం మరియు ఆందోళన

ప్రశ్న 9:

ఆన్‌లైన్ గ్రూమింగ్ భావనను పిల్లలు అర్థం చేసుకోవడం ఎందుకు అవసరం?

ఎ) పిల్లలు భయపడకుండా ఆన్‌లైన్ కార్యకలాపాల్లో పాల్గొనేలా ప్రోత్సహించడం

బి) పిల్లలను ఆన్‌లైన్ వస్త్రధారణకు మరింత హాని కలిగించేలా చేయడం

సి) సంభావ్య ప్రమాదాలను గుర్తించడానికి మరియు ఆన్‌లైన్‌లో తమను తాము రక్షించుకోవడానికి పిల్లలను శక్తివంతం చేయడం

డి) ఆన్‌లైన్‌లో ఇతరులతో వ్యక్తిగత సమాచారాన్ని ఉచితంగా పంచుకునేలా పిల్లలను ప్రోత్సహించడం

సమాధానం: సి) సంభావ్య ప్రమాదాలను గుర్తించడానికి మరియు ఆన్‌లైన్‌లో తమను తాము రక్షించుకోవడానికి పిల్లలను శక్తివంతం చేయడం

ప్రశ్న 10:

పిల్లలు ఆన్‌లైన్ వస్త్రధారణ ప్రవర్తనను ఎదుర్కొంటే ఏమి చేయాలి?

ఎ) స్నేహపూర్వక సంభాషణలో పాల్గొనండి మరియు ఆన్‌లైన్ గ్రూమర్‌తో కలిసి ఆడండి

బి) నమ్మకాన్ని పెంచుకోవడానికి ఆన్‌లైన్ గ్రూమర్‌తో వెంటనే వ్యక్తిగత సమాచారాన్ని షేర్ చేయండి

సి) ఆన్‌లైన్ గ్రూమర్‌తో కమ్యూనికేషన్‌ను ఆపివేసి, సంఘటనను విశ్వసనీయ పెద్దలకు నివేదించండి

డి) సరదాగా ఆన్‌లైన్ గ్రూమర్‌తో సన్నిహితంగా ఉండేలా స్నేహితులను ప్రోత్సహించండి

సమాధానం: సి) ఆన్‌లైన్ గ్రూమర్‌తో కమ్యూనికేషన్‌ను ఆపివేసి, సంఘటనను విశ్వసనీయ పెద్దలకు నివేదించండి

Day – 3

**ఇమెయిల్ బెదిరింపులు**

ప్రశ్న 1:

ఇమెయిల్ బెదిరింపులు ఏమిటి?

ఎ) స్నేహితులు మరియు కుటుంబ సభ్యులకు పంపబడిన జోకులు మరియు ఫన్నీ కథలతో కూడిన సందేశాలు

బి) ఆన్‌లైన్ భద్రత కోసం ఉపయోగకరమైన సమాచారం మరియు చిట్కాలను అందించే ఇమెయిల్‌లు

సి) హానికరమైన కంటెంట్‌ను కలిగి ఉన్న సందేశాలు మరియు గ్రహీతలకు ప్రమాదాలు ఉంటాయి

D) వ్యక్తిగత సమాచారాన్ని అభ్యర్థిస్తూ చట్టబద్ధమైన మూలాల నుండి ఇమెయిల్‌లు

సమాధానం: సి) హానికరమైన కంటెంట్‌ని కలిగి ఉన్న సందేశాలు మరియు గ్రహీతలకు ప్రమాదాలు ఉంటాయి

ప్రశ్న 2:

సున్నితమైన సమాచారాన్ని బహిర్గతం చేసేలా గ్రహీతలను మోసగించడానికి ఉపయోగించే ఇమెయిల్ బెదిరింపు యొక్క సాధారణ రకం ఏమిటి?

ఎ) ఫన్నీ కథనాలు మరియు చిత్రాలతో కూడిన గొలుసు ఇమెయిల్‌లు

బి) ఫిషింగ్ ఇమెయిల్‌లు నమ్మదగిన మూలాల నుండి వచ్చినట్లు నటించడం

సి) ఆన్‌లైన్ వార్తాలేఖల నుండి సబ్‌స్క్రిప్షన్ ఇమెయిల్‌లు

D) ఉపయోగకరమైన సమాచారాన్ని కలిగి ఉన్న పెద్ద జోడింపులతో ఇమెయిల్‌లు

సమాధానం: బి) నమ్మదగిన మూలాల నుండి వచ్చినట్లు నటిస్తూ ఫిషింగ్ ఇమెయిల్‌లు

ప్రశ్న 3:

ఫిషింగ్ ఇమెయిల్ యొక్క ప్రాథమిక లక్ష్యం ఏమిటి?

ఎ) సైబర్‌ సెక్యూరిటీ రిస్క్‌ల గురించి అవగాహన కల్పించడం

బి) ఆసక్తికరమైన కంటెంట్‌తో గ్రహీతలను అలరించడానికి

సి) పాస్‌వర్డ్‌లు లేదా ఆర్థిక డేటా వంటి సున్నితమైన సమాచారాన్ని పొందడానికి

D) రాబోయే ఆన్‌లైన్ ఈవెంట్‌ల గురించి గ్రహీతలకు తెలియజేయడానికి

సమాధానం: సి) పాస్‌వర్డ్‌లు లేదా ఆర్థిక డేటా వంటి సున్నితమైన సమాచారాన్ని పొందడానికి

ప్రశ్న 4:

తెలియని మూలాల నుండి వచ్చే ఇమెయిల్ జోడింపుల గురించి ఎందుకు జాగ్రత్తగా ఉండాలి?

ఎ) ఇమెయిల్ జోడింపులు ప్రమాదకరం మరియు బెదిరింపులను కలిగి ఉండవు

బి) తెలియని మూలాల నుండి ఇమెయిల్ జోడింపులు వైరస్లు లేదా మాల్వేర్లను కలిగి ఉండవచ్చు

సి) ఇమెయిల్ జోడింపులను సాధారణంగా స్నేహితులు మరియు కుటుంబ సభ్యులు మాత్రమే పంపుతారు

D) తెలియని మూలాల నుండి ఇమెయిల్ జోడింపులు ఎల్లప్పుడూ ఉపయోగకరమైన సమాచారాన్ని కలిగి ఉంటాయి

సమాధానం: బి) తెలియని మూలాల నుండి ఇమెయిల్ జోడింపులు వైరస్లు లేదా మాల్వేర్లను కలిగి ఉండవచ్చు

ప్రశ్న 5:

ఇమెయిల్ బెదిరింపుల సందర్భంలో "స్పూఫింగ్" అంటే ఏమిటి?

ఎ) అవాంఛిత ఇమెయిల్‌లు స్వీకర్త ఇన్‌బాక్స్‌కు చేరకుండా నిరోధించే టెక్నిక్

బి) స్నేహితులు మరియు కుటుంబ సభ్యులకు ఫన్నీ ఇమెయిల్‌లను ఫార్వార్డ్ చేసే చర్య

సి) గ్రహీతలను మోసం చేయడానికి చట్టబద్ధమైన ఇమెయిల్ పంపినవారి వలె నటించడం

D) వినోద ప్రయోజనాల కోసం నిర్దిష్ట క్రమంలో వరుస ఇమెయిల్‌లను పంపడం

సమాధానం: సి) గ్రహీతలను మోసం చేయడానికి చట్టబద్ధమైన ఇమెయిల్ పంపినవారి వలె నటించడం

ప్రశ్న 6:

మీరు లింక్ లేదా అటాచ్‌మెంట్‌తో అనుమానాస్పద ఇమెయిల్‌ను స్వీకరిస్తే మీరు ఏమి చేయాలి?

ఎ) లింక్‌పై క్లిక్ చేయండి లేదా అటాచ్‌మెంట్‌లో ఏమి ఉందో చూడటానికి దాన్ని తెరవండి

బి) స్నేహితులు మరియు కుటుంబ సభ్యుల అభిప్రాయాల కోసం ఇమెయిల్‌ను ఫార్వార్డ్ చేయండి

సి) మీ ఇమెయిల్ సర్వీస్ ప్రొవైడర్ లేదా IT విభాగానికి ఇమెయిల్‌ను నివేదించండి

D) ఇమెయిల్‌కు ప్రతిస్పందించండి మరియు మరింత సమాచారం కోసం అడగండి

సమాధానం: సి) మీ ఇమెయిల్ సర్వీస్ ప్రొవైడర్ లేదా IT విభాగానికి ఇమెయిల్‌ను నివేదించండి

ప్రశ్న 7:

"ransomware" ఇమెయిల్‌ల ప్రయోజనం ఏమిటి?

ఎ) స్వీకర్తలకు ఉచిత సాఫ్ట్‌వేర్ మరియు సాధనాలను అందించడం

బి) సైబర్‌ సెక్యూరిటీ బెదిరింపుల గురించి అవగాహన కల్పించడం

సి) బాధితుడి కంప్యూటర్‌లో ఫైల్‌లను డీక్రిప్ట్ చేయడానికి బదులుగా విమోచన చెల్లింపును అభ్యర్థించడం

డి) ఆన్‌లైన్ సర్వేలలో పాల్గొనడానికి గ్రహీతలను ప్రోత్సహించడం

సమాధానం: సి) బాధితుడి కంప్యూటర్‌లో ఫైల్‌లను డీక్రిప్ట్ చేయడానికి బదులుగా విమోచన చెల్లింపును అభ్యర్థించడం

ప్రశ్న 8:

సంభావ్య ఇమెయిల్ బెదిరింపులను మీరు ఎలా గుర్తించగలరు?

ఎ) మీ ఇన్‌బాక్స్‌లో వచ్చిన అన్ని ఇమెయిల్‌లను తెరిచి చదవడం ద్వారా

బి) పంపినవారి ఇమెయిల్ చిరునామాను ధృవీకరించడం మరియు అనుమానాస్పద అంశాల కోసం వెతకడం ద్వారా

సి) ప్రామాణికతను నిర్ధారించడానికి వ్యక్తిగత సమాచారం కోసం అడిగే ఇమెయిల్‌లకు ప్రతిస్పందించడం ద్వారా

D) వారి గమ్యాన్ని ధృవీకరించడానికి ఇమెయిల్‌లలోని లింక్‌లపై క్లిక్ చేయడం ద్వారా

సమాధానం: బి) పంపినవారి ఇమెయిల్ చిరునామాను ధృవీకరించడం మరియు అనుమానాస్పద అంశాల కోసం వెతకడం ద్వారా

ప్రశ్న 9:

మీరు అనుకోకుండా ఇమెయిల్‌లో అనుమానాస్పద లింక్‌పై క్లిక్ చేస్తే మీరు ఏమి చేయాలి?

ఎ) వెంటనే ఇమెయిల్‌ను మూసివేసి, సంఘటనను విస్మరించండి

బి) అసలు ఇమెయిల్‌కి తిరిగి నావిగేట్ చేయడానికి మరిన్ని లింక్‌లపై క్లిక్ చేయండి

సి) యాంటీవైరస్ సాఫ్ట్‌వేర్‌ని ఉపయోగించి పూర్తి సిస్టమ్ స్కాన్‌ను అమలు చేయండి

డి) పరిస్థితిని పరిష్కరించడానికి అభ్యర్థించిన వ్యక్తిగత సమాచారాన్ని అందించండి

సమాధానం: సి) యాంటీవైరస్ సాఫ్ట్‌వేర్‌ని ఉపయోగించి పూర్తి సిస్టమ్ స్కాన్‌ను అమలు చేయండి

ప్రశ్న 10:

ఇమెయిల్ బెదిరింపుల నుండి మిమ్మల్ని మీరు రక్షించుకోవడానికి ఉత్తమ మార్గం ఏమిటి?

ఎ) అన్ని ఇమెయిల్‌లను తెరిచి, వాటి కంటెంట్‌లను ధృవీకరించడానికి అన్ని లింక్‌లపై క్లిక్ చేయండి

బి) విశ్వాసాన్ని పెంపొందించడానికి పంపినవారితో వ్యక్తిగత సమాచారాన్ని ఉచితంగా పంచుకోండి

సి) ఇమెయిల్ ఖాతాల కోసం బలమైన మరియు ప్రత్యేకమైన పాస్‌వర్డ్‌లను ఉపయోగించండి

D) తెలియని మూలాల నుండి అన్ని ఇమెయిల్‌లను స్నేహితులు మరియు కుటుంబ సభ్యులకు ఫార్వార్డ్ చేయండి

సమాధానం: సి) ఇమెయిల్ ఖాతాల కోసం బలమైన మరియు ప్రత్యేకమైన పాస్‌వర్డ్‌లను ఉపయోగించండి

**పాస్‌వర్డ్ బెదిరింపులు:**

ప్రశ్న 1:

పాస్‌వర్డ్ బెదిరింపులు అంటే ఏమిటి?

ఎ) పాస్‌వర్డ్ భద్రతకు సంబంధించిన ఆన్‌లైన్ క్విజ్‌లు మరియు సవాళ్లు

బి) వారి పాస్‌వర్డ్‌లను ఉపయోగించి ఒకరి ఆన్‌లైన్ ఖాతాలను యాక్సెస్ చేయడానికి అనధికారిక ప్రయత్నాలు

సి) బలమైన మరియు ప్రత్యేకమైన పాస్‌వర్డ్‌లను సృష్టించే పాస్‌వర్డ్ జనరేటర్లు

D) లాగిన్ ఆధారాలను నిర్వహించడానికి పాస్‌వర్డ్ నిర్వహణ సాధనాలు

సమాధానం: బి) ఎవరైనా వారి పాస్‌వర్డ్‌లను ఉపయోగించి వారి ఆన్‌లైన్ ఖాతాలను యాక్సెస్ చేయడానికి అనధికారిక ప్రయత్నాలు

ప్రశ్న 2:

సరైన పాస్‌వర్డ్‌ని ఊహించడం కోసం అనేక విభిన్న పాస్‌వర్డ్ కాంబినేషన్‌లను ప్రయత్నించడం వల్ల తెలిసిన సాధారణ పాస్‌వర్డ్ ముప్పు ఏమిటి?

ఎ) సోషల్ ఇంజనీరింగ్

బి) బ్రూట్-ఫోర్స్ దాడి

సి) రెండు-కారకాల ప్రమాణీకరణ

డి) పాస్‌వర్డ్ ఎన్‌క్రిప్షన్

జవాబు: బి) బ్రూట్-ఫోర్స్ దాడి

ప్రశ్న 3:

విభిన్న ఆన్‌లైన్ ఖాతాల కోసం బలమైన మరియు ప్రత్యేకమైన పాస్‌వర్డ్‌లను ఉపయోగించడం ఎందుకు అవసరం?

ఎ) పాస్‌వర్డ్ సంక్లిష్టతతో ఇతరులను ఆకట్టుకోవడానికి

బి) పాస్‌వర్డ్‌లను సులభంగా గుర్తుంచుకోవడానికి

సి) ఒక పాస్‌వర్డ్ రాజీపడితే బహుళ ఖాతాలకు అనధికారిక యాక్సెస్‌ను నిరోధించడం

డి) పాస్‌వర్డ్ సృజనాత్మకత మరియు ఆవిష్కరణలను ప్రదర్శించడానికి

సమాధానం: సి) ఒక పాస్‌వర్డ్ రాజీ పడినట్లయితే బహుళ ఖాతాలకు అనధికార ప్రాప్యతను నిరోధించడానికి

ప్రశ్న 4:

పాస్‌వర్డ్ బెదిరింపుల సందర్భంలో "పాస్‌వర్డ్ క్రాకింగ్" అంటే ఏమిటి?

ఎ) భద్రతను మెరుగుపరచడానికి పాస్‌వర్డ్‌లను తరచుగా మార్చే ప్రక్రియ

బి) స్నేహితులు లేదా కుటుంబ సభ్యులతో పాస్‌వర్డ్‌లను పంచుకునే చర్య

సి) పాస్‌వర్డ్‌లను అనధికార యాక్సెస్ నుండి రక్షించడానికి ఎన్‌క్రిప్షన్‌ని ఉపయోగించడం

డి) అధికారం లేకుండా పాస్‌వర్డ్‌లను కనుగొనడానికి లేదా డీకోడ్ చేయడానికి వివిధ పద్ధతులను ఉపయోగించడం

జవాబు: D) అధికారం లేకుండా పాస్‌వర్డ్‌లను కనుగొనడానికి లేదా డీకోడ్ చేయడానికి వివిధ పద్ధతులను ఉపయోగించడం

ప్రశ్న 5:

పాస్‌వర్డ్ బెదిరింపులకు సంబంధించిన "ఫిషింగ్" అంటే ఏమిటి?

ఎ) స్నేహితులు మరియు కుటుంబ సభ్యులకు ఫన్నీ ఇమెయిల్‌లను పంపడం

బి) సోషల్ మీడియాలో స్ఫూర్తిదాయకమైన కోట్స్ మరియు చిత్రాలను పంచుకోవడం

సి) వ్యక్తులు తమ పాస్‌వర్డ్‌లను బహిర్గతం చేయడానికి నకిలీ ఇమెయిల్‌లు లేదా సందేశాలను పంపడం

డి) ఆన్‌లైన్ ఖాతాల కోసం సంక్లిష్టమైన పాస్‌వర్డ్‌లను రూపొందించడం

జవాబు: సి) వ్యక్తులు తమ పాస్‌వర్డ్‌లను బహిర్గతం చేసేందుకు నకిలీ ఇమెయిల్‌లు లేదా సందేశాలను పంపడం

ప్రశ్న 6:

"పాస్‌వర్డ్" లేదా "123456" వంటి సాధారణ పాస్‌వర్డ్‌లను ఉపయోగించడం ఎందుకు చెడు పద్ధతి?

ఎ) సాధారణ పాస్‌వర్డ్‌లు గుర్తుంచుకోవడం సులభం

బి) సాధారణ పాస్‌వర్డ్‌లను ఉపయోగించడం వల్ల హ్యాకర్లు వాటిని ఊహించడం కష్టతరం చేస్తుంది

సి) పాస్‌వర్డ్ క్రాకింగ్ సాధనాలను ఉపయోగించి సాధారణ పాస్‌వర్డ్‌లను క్రాక్ చేయడం కష్టం

D) హ్యాకర్లు తరచుగా సాధారణ పాస్‌వర్డ్‌లతో ఖాతాలను లక్ష్యంగా చేసుకుంటారు, వాటిని హాని కలిగి ఉంటారు

జవాబు: D) హ్యాకర్లు తరచుగా సాధారణ పాస్‌వర్డ్‌లతో ఖాతాలను లక్ష్యంగా చేసుకుంటారు, వాటిని హాని కలిగి ఉంటారు

ప్రశ్న 7:

పాస్‌వర్డ్ భద్రతలో "పాస్‌వర్డ్ మేనేజర్‌ల" ప్రయోజనం ఏమిటి?

ఎ) అన్ని ఆన్‌లైన్ ఖాతాల కోసం యాదృచ్ఛిక పాస్‌వర్డ్‌లను రూపొందించడానికి

బి) లాగిన్ ఆధారాలను సురక్షితంగా నిల్వ చేయడానికి మరియు నిర్వహించడానికి

సి) స్నేహితులు మరియు కుటుంబ సభ్యులతో పాస్‌వర్డ్‌లను పంచుకోవడానికి

D) అనధికార యాక్సెస్‌ను నిరోధించడానికి పాస్‌వర్డ్‌లను తరచుగా మార్చడం

సమాధానం: బి) లాగిన్ ఆధారాలను సురక్షితంగా నిల్వ చేయడానికి మరియు నిర్వహించడానికి

ప్రశ్న 8:

పాస్‌వర్డ్‌లలో మీ పేరు లేదా పుట్టిన తేదీ వంటి వ్యక్తిగత సమాచారాన్ని ఎందుకు ఉపయోగించకుండా ఉండాలి?

ఎ) వ్యక్తిగత సమాచారాన్ని గుర్తుంచుకోవడం సులభం

బి) వ్యక్తిగత సమాచారం పాస్‌వర్డ్‌లను మరింత ప్రత్యేకంగా చేస్తుంది

C) దాడి చేసేవారు వ్యక్తిగత సమాచారాన్ని సులభంగా కనుగొనవచ్చు లేదా ఊహించవచ్చు

డి) వ్యక్తిగత సమాచారం పాస్‌వర్డ్ సంక్లిష్టతను పెంచుతుంది

సమాధానం: సి) దాడి చేసేవారు వ్యక్తిగత సమాచారాన్ని సులభంగా కనుగొనవచ్చు లేదా ఊహించవచ్చు

ప్రశ్న 9:

పాస్‌వర్డ్ బెదిరింపుల సందర్భంలో "క్రెడెన్షియల్ స్టఫింగ్" అంటే ఏమిటి?

ఎ) బహుళ ఆన్‌లైన్ సేవలతో పాస్‌వర్డ్‌లను పంచుకునే చర్య

బి) బహుళ ఖాతాల కోసం ఒకే పాస్‌వర్డ్‌ను మళ్లీ ఉపయోగించడం

సి) సాధారణ పదబంధాలు మరియు నమూనాలను ఉపయోగించి పాస్‌వర్డ్‌లను అంచనా వేయడానికి ప్రయత్నించడం

డి) వివిధ వెబ్‌సైట్‌లలో దొంగిలించబడిన వినియోగదారు పేరు/పాస్‌వర్డ్ కలయికలను ప్రయత్నించడానికి ఆటోమేటెడ్ సాధనాలను ఉపయోగించడం

సమాధానం: డి) వివిధ వెబ్‌సైట్‌లలో దొంగిలించబడిన వినియోగదారు పేరు/పాస్‌వర్డ్ కలయికలను ప్రయత్నించడానికి ఆటోమేటెడ్ సాధనాలను ఉపయోగించడం

ప్రశ్న 10:

పాస్‌వర్డ్ బెదిరింపుల నుండి మిమ్మల్ని మీరు ఎలా రక్షించుకోవచ్చు?

ఎ) బ్యాకప్ కోసం మీ పాస్‌వర్డ్‌లను స్నేహితులు మరియు కుటుంబ సభ్యులతో పంచుకోవడం

బి) సౌలభ్యం కోసం సులభమైన మరియు సులభంగా గుర్తుంచుకోగల పాస్‌వర్డ్‌లను ఉపయోగించడం

సి) ఆన్‌లైన్ ఖాతాల కోసం రెండు-కారకాల ప్రమాణీకరణను ప్రారంభించడం

డి) భద్రంగా ఉంచుకోవడానికి పాస్‌వర్డ్‌లను కాగితంపై రాయడం

సమాధానం: సి) ఆన్‌లైన్ ఖాతాల కోసం రెండు-కారకాల ప్రమాణీకరణను ప్రారంభించడం

**క్రెడిట్ కార్డ్ మోసాలు:**

ప్రశ్న 1:

క్రెడిట్ కార్డ్ స్కామ్‌లు అంటే ఏమిటి?

ఎ) క్రెడిట్ కార్డ్ కంపెనీలు అందించే చట్టబద్ధమైన ప్రమోషన్‌లు మరియు తగ్గింపులు

బి) క్రెడిట్ కార్డ్ లావాదేవీల సమయంలో అనుకోని తప్పులు జరుగుతాయి

సి) మోసపూరిత ప్రయోజనాల కోసం క్రెడిట్ కార్డ్ సమాచారాన్ని దొంగిలించడానికి ఉద్దేశించిన మోసపూరిత పద్ధతులు

D) ఎటువంటి అదనపు ధృవీకరణ లేకుండా క్రెడిట్ కార్డ్ పరిమితులను పెంచడానికి ఆఫర్ చేస్తుంది

జవాబు: సి) మోసపూరిత ప్రయోజనాల కోసం క్రెడిట్ కార్డ్ సమాచారాన్ని దొంగిలించడానికి ఉద్దేశించిన మోసపూరిత పద్ధతులు

ప్రశ్న 2:

క్రెడిట్ కార్డ్ స్కామ్‌ల సందర్భంలో "క్రెడిట్ కార్డ్ ఫిషింగ్" అంటే ఏమిటి?

ఎ) కోల్పోయిన లేదా దొంగిలించబడిన క్రెడిట్ కార్డ్‌లను జారీ చేసేవారికి నివేదించే ప్రక్రియ

బి) క్రెడిట్ కార్డ్ కంపెనీలతో తక్కువ వడ్డీ రేట్లను చర్చించడానికి ఒక సాంకేతికత

సి) క్రెడిట్ కార్డ్ సమాచారాన్ని బహిర్గతం చేయడానికి వ్యక్తులను మోసగించడానికి చట్టబద్ధమైన సంస్థలుగా నటిస్తూ నకిలీ ఇమెయిల్‌లు లేదా సందేశాలను పంపడం

D) క్రెడిట్ కార్డులను ఉపయోగించి నగదు అడ్వాన్స్‌లను పొందే వ్యూహం

జవాబు: సి) క్రెడిట్ కార్డ్ సమాచారాన్ని బహిర్గతం చేయడానికి వ్యక్తులను మోసగించడానికి చట్టబద్ధమైన సంస్థలుగా నటిస్తూ నకిలీ ఇమెయిల్‌లు లేదా సందేశాలను పంపడం

ప్రశ్న 3:

క్రెడిట్ కార్డ్ స్కిమ్మింగ్ ఎలా జరుగుతుంది?

ఎ) క్రెడిట్ కార్డ్ కంపెనీల నుండి ప్రమోషనల్ ఆఫర్‌లను స్వీకరించడం ద్వారా

బి) క్రెడిట్ కార్డ్ స్టేట్‌మెంట్‌లో అనధికార లావాదేవీలు కనిపించినప్పుడు

సి) చట్టబద్ధమైన లావాదేవీల సమయంలో క్రెడిట్ కార్డ్ సమాచారాన్ని సంగ్రహించడానికి కార్డ్ రీడర్‌లలో పరికరాలను ఇన్‌స్టాల్ చేయడం ద్వారా

D) అయస్కాంతాలను ఉపయోగించి మాగ్నెటిక్ స్ట్రిప్ నుండి క్రెడిట్ కార్డ్ సమాచారాన్ని పొందడం ద్వారా

సమాధానం: సి) చట్టబద్ధమైన లావాదేవీల సమయంలో క్రెడిట్ కార్డ్ సమాచారాన్ని సంగ్రహించడానికి కార్డ్ రీడర్‌లలో పరికరాలను ఇన్‌స్టాల్ చేయడం ద్వారా

ప్రశ్న 4:

క్రెడిట్ కార్డ్ స్కామ్ యొక్క సాధారణ హెచ్చరిక సంకేతం ఏమిటి?

ఎ) క్రెడిట్ కార్డ్ కంపెనీ అనధికార ఛార్జీల గురించి కార్డ్ హోల్డర్‌కు తెలియజేస్తుంది

B) క్రెడిట్ కార్డ్ అప్‌గ్రేడ్‌ల కోసం చట్టబద్ధమైన కంపెనీల నుండి తరచుగా ఆఫర్‌లు

సి) ఆకర్షణీయమైన క్రెడిట్ కార్డ్ డీల్‌లతో ప్రచార ఇమెయిల్‌లను స్వీకరించడం

D) క్రెడిట్ కార్డ్ స్టేట్‌మెంట్‌లో కనిపించే అసాధారణమైన లేదా తెలియని ఛార్జీలు

జవాబు: D) క్రెడిట్ కార్డ్ స్టేట్‌మెంట్‌లో కనిపించే అసాధారణమైన లేదా తెలియని ఛార్జీలు

ప్రశ్న 5:

ఆన్‌లైన్ లావాదేవీల సమయంలో క్రెడిట్ కార్డ్ సమాచారాన్ని రక్షించడం ఎందుకు అవసరం?

ఎ) క్రెడిట్ కార్డ్ కంపెనీలు అదనపు రుసుములు వసూలు చేయవని నిర్ధారించడానికి

బి) కోల్పోయిన క్రెడిట్ కార్డ్‌ను భర్తీ చేయడం వల్ల కలిగే అసౌకర్యాన్ని నివారించడానికి

C) క్రెడిట్ కార్డ్ సమాచారం స్కామర్ల చేతుల్లోకి రాకుండా నిరోధించడం

D) క్రెడిట్ కార్డ్ రివార్డ్ ప్రోగ్రామ్‌లలో పాల్గొనడానికి

జవాబు: సి) క్రెడిట్ కార్డ్ సమాచారం స్కామర్ల చేతుల్లోకి రాకుండా నిరోధించడానికి

ప్రశ్న 6:

మీరు క్రెడిట్ కార్డ్ స్కామ్‌కు గురైనట్లు అనుమానించినట్లయితే మీరు ఏమి చేయాలి?

ఎ) అనుమానాస్పద ఛార్జీలను విస్మరించండి మరియు అవి అదృశ్యమయ్యే వరకు వేచి ఉండండి

బి) మీ క్రెడిట్ కార్డ్ కంపెనీకి అనుమానాస్పద ఛార్జీలను వెంటనే నివేదించండి మరియు కొత్త కార్డ్‌ని అభ్యర్థించండి

సి) సలహా కోసం మీ క్రెడిట్ కార్డ్ సమాచారాన్ని స్నేహితులు లేదా కుటుంబ సభ్యులతో పంచుకోండి

D) సమస్యను పరిష్కరిస్తానని వాగ్దానం చేసే మూడవ పక్ష సేవలకు మీ క్రెడిట్ కార్డ్ సమాచారాన్ని అందించండి

సమాధానం: బి) మీ క్రెడిట్ కార్డ్ కంపెనీకి అనుమానాస్పద ఛార్జీలను వెంటనే నివేదించండి మరియు కొత్త కార్డ్ కోసం అభ్యర్థించండి

ప్రశ్న 7:

ఆన్‌లైన్ కొనుగోళ్లు చేసేటప్పుడు క్రెడిట్ కార్డ్ స్కామ్‌ల నుండి మిమ్మల్ని మీరు ఎలా రక్షించుకోవచ్చు?

ఎ) సజావుగా లావాదేవీలు జరిగేలా ప్రతి వెబ్‌సైట్‌కి మీ క్రెడిట్ కార్డ్ సమాచారాన్ని అందించడం

బి) అతి తక్కువ ధరలు మరియు ఉత్తమమైన డీల్‌లతో వెబ్‌సైట్‌లలో మాత్రమే షాపింగ్ చేయండి

సి) ఆన్‌లైన్ కొనుగోళ్ల కోసం ఎన్‌క్రిప్టెడ్ కనెక్షన్‌లతో సురక్షితమైన మరియు ప్రసిద్ధ వెబ్‌సైట్‌లను ఉపయోగించడం

D) సౌలభ్యం కోసం సోషల్ మీడియాలో మీ క్రెడిట్ కార్డ్ సమాచారాన్ని పంచుకోవడం

సమాధానం: సి) ఆన్‌లైన్ కొనుగోళ్ల కోసం ఎన్‌క్రిప్టెడ్ కనెక్షన్‌లతో సురక్షితమైన మరియు ప్రసిద్ధ వెబ్‌సైట్‌లను ఉపయోగించడం

ప్రశ్న 8:

క్రెడిట్ కార్డ్ స్కామ్‌ల సందర్భంలో "కార్డింగ్" అంటే ఏమిటి?

ఎ) అనధికార ఛార్జీలను నివారించడానికి క్రెడిట్ కార్డ్‌ను రద్దు చేసే చర్య

బి) క్రెడిట్ కార్డ్ సమాచారాన్ని చట్టవిరుద్ధంగా పొందడం మరియు మోసపూరిత ప్రయోజనాల కోసం ఉపయోగించడం

సి) రివార్డ్‌లు మరియు క్యాష్‌బ్యాక్ సంపాదించడానికి క్రెడిట్ కార్డ్‌లను ఉపయోగించే పద్ధతి

D) క్రెడిట్ పరిమితులను పెంచడానికి బహుళ క్రెడిట్ కార్డ్‌ల కోసం దరఖాస్తు చేసే చర్య

జవాబు: బి) క్రెడిట్ కార్డ్ సమాచారాన్ని చట్టవిరుద్ధంగా పొందడం మరియు మోసపూరిత ప్రయోజనాల కోసం ఉపయోగించడం

ప్రశ్న 9:

క్రెడిట్ కార్డ్ స్టేట్‌మెంట్‌లను క్రమం తప్పకుండా సమీక్షించడం ఎందుకు ముఖ్యం?

ఎ) క్రెడిట్ కార్డ్ రివార్డ్‌లు మరియు బోనస్‌లను ట్రాక్ చేయడానికి

బి) అనధికార ఛార్జీలు లేదా అనుమానాస్పద కార్యకలాపాలను గుర్తించడం

సి) క్రెడిట్ కార్డ్ కంపెనీతో చట్టబద్ధమైన ఛార్జీలను వివాదం చేయడానికి

D) అన్ని క్రెడిట్ కార్డ్ లావాదేవీలపై క్యాష్‌బ్యాక్ సంపాదించడానికి

జవాబు: బి) అనధికార ఛార్జీలు లేదా అనుమానాస్పద కార్యకలాపాలను గుర్తించడం

ప్రశ్న 10:

మీ క్రెడిట్ కార్డ్ సమాచారం కోసం మీకు ఫోన్ కాల్ లేదా ఇమెయిల్ వస్తే మీరు ఏమి చేయాలి?

ఎ) ఏవైనా సంభావ్య సమస్యలను నివారించడానికి అభ్యర్థించిన సమాచారాన్ని అందించండి

బి) అభ్యర్థనను తిరస్కరించండి మరియు ఇమెయిల్‌ను హ్యాంగ్ అప్ చేయండి లేదా తొలగించండి

సి) అభ్యర్థన యొక్క చట్టబద్ధతను నిర్ధారించడానికి క్రెడిట్ కార్డ్ కంపెనీకి కాల్ చేయండి

డి) కాలర్ లేదా పంపినవారు ప్రభుత్వ అధికారి అని క్లెయిమ్ చేసుకుంటే మాత్రమే సమాచారాన్ని షేర్ చేయండి

సమాధానం: బి) అభ్యర్థనను తిరస్కరించండి మరియు ఇమెయిల్‌ను హ్యాంగ్ అప్ చేయండి లేదా తొలగించండి

**ఇమెయిల్ లాటరీ మోసాలు**

ప్రశ్న 1:

ఇమెయిల్ లాటరీ అంటే ఏమిటి?

ఎ) ఇమెయిల్ ద్వారా నిర్వహించబడిన మరియు నిర్వహించబడే చట్టబద్ధమైన లాటరీ

B) పాల్గొనేవారు ఇమెయిల్ ద్వారా లాటరీ గేమ్‌లు ఆడే వినోదం యొక్క ఒక రూపం

సి) గ్రహీత లాటరీ బహుమతిని గెలుచుకున్నారని క్లెయిమ్ చేసే మోసపూరిత ఇమెయిల్ స్కామ్

D) ఇమెయిల్ చందాదారుల కోసం ప్రత్యేకంగా లాటరీ

సమాధానం: సి) గ్రహీత లాటరీ బహుమతిని గెలుచుకున్నారని మోసపూరిత ఇమెయిల్ స్కామ్

ప్రశ్న 2:

ఇమెయిల్ లాటరీ స్కామ్‌లలో స్వీకర్తలను మోసగించడానికి ఉపయోగించే సాధారణ వ్యూహం ఏమిటి?

ఎ) ఇమెయిల్ ద్వారా అధికారిక లాటరీ టిక్కెట్లను పంపడం

బి) లాటరీ విజయాల గురించి ఖచ్చితమైన సమాచారాన్ని అందించడం

సి) అనుకున్న బహుమతిని క్లెయిమ్ చేయడానికి వ్యక్తిగత సమాచారం మరియు చెల్లింపును అభ్యర్థించడం

D) భవిష్యత్ డ్రాయింగ్‌ల కోసం ఉచిత లాటరీ ఎంట్రీలను అందిస్తోంది

సమాధానం: సి) అనుకున్న బహుమతిని క్లెయిమ్ చేయడానికి వ్యక్తిగత సమాచారం మరియు చెల్లింపును అభ్యర్థించడం

ప్రశ్న 3:

ఇమెయిల్ లాటరీ స్కామ్‌లు సాధారణంగా గ్రహీతలకు వారి విజయాల గురించి ఎలా తెలియజేస్తాయి?

ఎ) వారి మెయిలింగ్ చిరునామాకు భౌతిక లేఖలను పంపడం ద్వారా

బి) విజయాల గురించి వారికి తెలియజేయడానికి ఫోన్ కాల్స్ చేయడం ద్వారా

సి) సోషల్ మీడియా ప్లాట్‌ఫారమ్‌ల ద్వారా వారిని సంప్రదించడం ద్వారా

D) లాటరీ బహుమతులను గెలుచుకున్నట్లు తప్పుడు వాదనలతో ఇమెయిల్‌లను పంపడం ద్వారా

సమాధానం: D) లాటరీ బహుమతులు గెలుచుకున్న తప్పుడు వాదనలతో ఇమెయిల్‌లను పంపడం ద్వారా

ప్రశ్న 4:

లాటరీ విజయాలను క్లెయిమ్ చేసే ఇమెయిల్‌ల విషయంలో జాగ్రత్తగా ఉండటం ఎందుకు అవసరం?

ఎ) ఇమెయిల్ ద్వారా లాటరీ బహుమతులు గెలవడం ఒక సాధారణ పద్ధతి

బి) ఎలాంటి ప్రమాదాలు లేకుండా త్వరగా ధనవంతులు కావడానికి ఇది సులభమైన మార్గం

సి) చాలా ఇమెయిల్ లాటరీ క్లెయిమ్‌లు చట్టబద్ధమైనవి మరియు ధృవీకరించబడినవి

D) ఇమెయిల్ లాటరీ స్కామ్‌లు గ్రహీతలను మోసం చేయడానికి మరియు మోసం చేయడానికి రూపొందించబడ్డాయి

సమాధానం: డి) ఇమెయిల్ లాటరీ స్కామ్‌లు గ్రహీతలను మోసం చేయడానికి మరియు మోసం చేయడానికి రూపొందించబడ్డాయి

ప్రశ్న 5:

మీరు లాటరీ బహుమతిని గెలుచుకున్నట్లు క్లెయిమ్ చేస్తూ మీకు ఇమెయిల్ వస్తే, మీరు ఏ లాటరీలోనూ పాల్గొనకపోతే ఏమి చేయాలి?

ఎ) స్నేహితులు మరియు కుటుంబ సభ్యులతో వారి అభిప్రాయాల కోసం ఇమెయిల్‌ను పంచుకోండి

బి) ఇమెయిల్‌కు ప్రతిస్పందించండి మరియు ధృవీకరణ కోసం అభ్యర్థించిన సమాచారాన్ని అందించండి

సి) ఇమెయిల్‌ను విస్మరించండి మరియు వెంటనే దాన్ని తొలగించండి

D) బహుమతి వివరాలను ధృవీకరించడానికి ఇమెయిల్‌లోని ఏవైనా లింక్‌లపై క్లిక్ చేయండి

సమాధానం: సి) ఇమెయిల్‌ను విస్మరించండి మరియు వెంటనే దాన్ని తొలగించండి

ప్రశ్న 6:

వ్యక్తిగత సమాచారం మరియు చెల్లింపు కోసం అడిగే ఇమెయిల్ లాటరీ స్కామ్‌ల ప్రయోజనం ఏమిటి?

ఎ) భవిష్యత్తులో లాటరీలలో స్వయంచాలకంగా గ్రహీతను నమోదు చేయడానికి

బి) బహుమతికి గ్రహీత యొక్క గుర్తింపు మరియు అర్హతను ధృవీకరించడానికి

సి) గ్రహీత యొక్క వ్యక్తిగత సమాచారాన్ని చట్టబద్ధమైన లాటరీ నిర్వాహకులతో పంచుకోవడానికి

D) గ్రహీతను మోసం చేయడం మరియు వారి డబ్బు లేదా గుర్తింపును దొంగిలించడం

సమాధానం: D) గ్రహీతను మోసం చేయడం మరియు వారి డబ్బు లేదా గుర్తింపును దొంగిలించడం

ప్రశ్న 7:

ఇమెయిల్ లాటరీ స్కామ్‌ల యొక్క కొన్ని రెడ్ ఫ్లాగ్‌లు ఏమిటి?

ఎ) గ్రహీతను పేరు ద్వారా సంబోధించే వ్యక్తిగతీకరించిన ఇమెయిల్‌లు

బి) లాటరీ బహుమతిని క్లెయిమ్ చేయడానికి చెల్లింపు కోసం అభ్యర్థనలు

సి) అధికారిక లాటరీ సంస్థలకు సరిపోలే ఇమెయిల్ చిరునామాలు

D) బాగా తెలిసిన మరియు చట్టబద్ధమైన లాటరీ లోగోలు మరియు బ్రాండింగ్ యొక్క ఉపయోగం

సమాధానం: బి) లాటరీ బహుమతిని క్లెయిమ్ చేయడానికి చెల్లింపు కోసం అభ్యర్థనలు

ప్రశ్న 8:

లాటరీ బహుమతిని అత్యవసరంగా క్లెయిమ్ చేయాలని స్కామర్‌లు ఎందుకు తరచుగా పేర్కొంటారు?

ఎ) గ్రహీతను ఆలోచించకుండా త్వరగా పని చేయమని ఒత్తిడి చేయడం

బి) మరొకరు క్లెయిమ్ చేసే ముందు బహుమతి సురక్షితంగా ఉందని నిర్ధారించుకోవడం

సి) బహుమతి విజేతకు మెరుగైన కస్టమర్ సేవను అందించడం

D) ఇమెయిల్ యొక్క చట్టబద్ధతను ధృవీకరించడానికి స్వీకర్తకు తగినంత సమయాన్ని అనుమతించడం

జవాబు: ఎ) గ్రహీతను ఆలోచించకుండా త్వరగా పని చేసేలా ఒత్తిడి చేయడం

ప్రశ్న 9:

మీరు ఇమెయిల్ లాటరీ స్కామ్‌ను అందుకున్నారని మీరు అనుమానించినట్లయితే మీరు ఏమి చేయాలి?

ఎ) మీ ఇమెయిల్ సర్వీస్ ప్రొవైడర్‌కు ఇమెయిల్‌ను నివేదించండి

బి) స్నేహితులు మరియు కుటుంబ సభ్యులతో వారి అభిప్రాయాల కోసం ఇమెయిల్‌ను పంచుకోండి

సి) ఇమెయిల్‌కు ప్రతిస్పందించండి మరియు బహుమతి గురించి మరింత సమాచారం కోసం అడగండి

D) బహుమతిని క్లెయిమ్ చేయడానికి అభ్యర్థించినట్లుగా మీ వ్యక్తిగత సమాచారాన్ని అందించండి

సమాధానం: ఎ) మీ ఇమెయిల్ సర్వీస్ ప్రొవైడర్‌కు ఇమెయిల్‌ను నివేదించండి

ప్రశ్న 10:

ఇమెయిల్ లాటరీ స్కామ్‌ల గురించి ఇతరులకు అవగాహన కల్పించడం ఎందుకు అవసరం?

ఎ) తాజా లాటరీ గేమ్‌లు మరియు ప్రమోషన్‌ల గురించి ప్రజలకు అవగాహన కల్పించడం

బి) చట్టబద్ధమైన లాటరీలలో పాల్గొనడానికి ఇతరులను ప్రోత్సహించడం

సి) మోసాలు మరియు ఆర్థిక నష్టాల బారిన పడకుండా ఇతరులను నిరోధించడం

D) ఇమెయిల్ లాటరీల భావనను చట్టబద్ధమైన వినోద రూపంగా ప్రచారం చేయడం

జవాబు: సి) మోసాలు మరియు ఆర్థిక నష్టాల బారిన పడకుండా ఇతరులను నిరోధించడం

**సైబర్ బెదిరింపు**

ప్రశ్న 1: కింది వాటిలో సైబర్ బెదిరింపును ఏది ఉత్తమంగా నిర్వచిస్తుంది?

ఎ) సానుకూల ఆన్‌లైన్ పరస్పర చర్యలను ప్రోత్సహించడం.

బి) ఆన్‌లైన్ భద్రతను ప్రోత్సహించే చర్య.

సి) ఇతరులను వేధించడానికి, భయపెట్టడానికి లేదా హాని చేయడానికి డిజిటల్ కమ్యూనికేషన్‌ను ఉపయోగించడం.

డి) సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లలో ఆలోచనలు మరియు అభిప్రాయాల మార్పిడి.

జవాబు: సి) ఇతరులను వేధించడానికి, భయపెట్టడానికి లేదా హాని చేయడానికి డిజిటల్ కమ్యూనికేషన్‌ను ఉపయోగించడం.

ప్రశ్న 2: సాంప్రదాయ బెదిరింపు నుండి సైబర్ బెదిరింపు ఎలా భిన్నంగా ఉంటుంది?

ఎ) సైబర్ బెదిరింపు శారీరక హానిని కలిగి ఉంటుంది, అయితే సాంప్రదాయ బెదిరింపు కేవలం మాటలతో మాత్రమే ఉంటుంది.

బి) సైబర్ బెదిరింపు ఆన్‌లైన్‌లో జరుగుతుంది, అయితే సాంప్రదాయ బెదిరింపు వ్యక్తిగతంగా జరుగుతుంది.

సి) సైబర్ బెదిరింపు ఎల్లప్పుడూ అపరిచితులచే చేయబడుతుంది, అయితే సాంప్రదాయ బెదిరింపు పరిచయస్తులచే చేయబడుతుంది.

డి) సాంప్రదాయ బెదిరింపు కంటే సైబర్ బెదిరింపు తక్కువ హానికరం.

సమాధానం: బి) సైబర్ బెదిరింపు ఆన్‌లైన్‌లో జరుగుతుంది, అయితే సాంప్రదాయ బెదిరింపు వ్యక్తిగతంగా జరుగుతుంది.

ప్రశ్న 3: కింది రకాల సైబర్ బెదిరింపులలో ఏది సర్వసాధారణం?

ఎ) టెక్స్ట్ లేదా సోషల్ మీడియా ద్వారా అభ్యంతరకరమైన సందేశాలను పంపడం.

బి) ఒకరిలా నటించి, తప్పుడు సమాచారాన్ని వ్యాప్తి చేయడానికి నకిలీ ప్రొఫైల్‌లను సృష్టించడం.

సి) పబ్లిక్ ఫోరమ్‌లు లేదా సోషల్ మీడియాలో బాధించే వ్యాఖ్యలను పోస్ట్ చేయడం.

డి) ఆన్‌లైన్‌లో వాదనలు లేదా విభేదాలలో పాల్గొనడం.

జవాబు: ఎ) టెక్స్ట్ లేదా సోషల్ మీడియా ద్వారా అభ్యంతరకరమైన సందేశాలను పంపడం.

ప్రశ్న 4: సైబర్ బెదిరింపు బాధితుడి మానసిక ఆరోగ్యాన్ని ఎలా ప్రభావితం చేస్తుంది?

ఎ) ఇది మానసిక ఆరోగ్యంపై ఎటువంటి ప్రభావం చూపదు, శారీరక శ్రేయస్సుపై మాత్రమే.

బి) బాధితులు ఆందోళన, నిరాశ లేదా తక్కువ ఆత్మగౌరవాన్ని అనుభవించవచ్చు.

సి) సైబర్ బెదిరింపు మెరుగైన స్థితిస్థాపకత మరియు కోపింగ్ నైపుణ్యాలకు దారితీస్తుంది.

డి) సైబర్ బెదిరింపు బాధితుడి సామాజిక జీవితాన్ని మాత్రమే ప్రభావితం చేస్తుంది, వారి మానసిక ఆరోగ్యంపై కాదు.

సమాధానం: బి) బాధితులు ఆందోళన, నిరాశ లేదా తక్కువ ఆత్మగౌరవాన్ని అనుభవించవచ్చు.

ప్రశ్న 5: సైబర్ బెదిరింపును ఎదుర్కోవడానికి కొన్ని ప్రభావవంతమైన మార్గాలు ఏమిటి?

ఎ) దూకుడు భాష మరియు బెదిరింపులతో ప్రతిస్పందించడం.

బి) సైబర్ బెదిరింపును విస్మరించడం మరియు అది దానంతటదే ఆగిపోతుందని ఆశించడం.

సి) సంఘటనను తగిన ప్లాట్‌ఫారమ్ లేదా అధికారానికి నివేదించడం.

డి) దురాక్రమణదారుపై సైబర్ బెదిరింపులో పాల్గొనడం ద్వారా ప్రతీకారం తీర్చుకోవడం.

సమాధానం: సి) సంఘటనను తగిన ప్లాట్‌ఫారమ్ లేదా అధికారానికి నివేదించడం.

ప్రశ్న 6: సైబర్ బెదిరింపును నిరోధించడంలో ప్రేక్షకులు ఏ పాత్ర పోషిస్తారు?

ఎ) పరిస్థితిని విస్మరించడం మరియు జోక్యం చేసుకోకపోవడం.

బి) సైబర్ బెదిరింపు ప్రవర్తనను కొనసాగించమని ప్రోత్సహించడం.

సి) సంఘటనను నివేదించడం మరియు బాధితునికి సహాయం అందించడం.

డి) అవగాహన పెంచడానికి సైబర్ బెదిరింపు కంటెంట్‌ను పంచుకోవడం.

సమాధానం: సి) సంఘటనను నివేదించడం మరియు బాధితునికి సహాయం అందించడం.

ప్రశ్న 7: సైబర్ బెదిరింపు గురించి అవగాహన పెంచుకోవడం ఎందుకు అవసరం?

ఎ) మరిన్ని ఆన్‌లైన్ డిబేట్‌లలో పాల్గొనేలా ప్రజలను ప్రోత్సహించడం.

బి) సోషల్ మీడియాను ఎలా సమర్థవంతంగా ఉపయోగించాలో అందరికీ తెలుసునని నిర్ధారించడానికి.

సి) ఆన్‌లైన్ పరస్పర చర్యలలో తాదాత్మ్యం మరియు దయను ప్రోత్సహించడం.

D) ఇంటర్నెట్ మరియు డిజిటల్ కమ్యూనికేషన్ వినియోగాన్ని నిరుత్సాహపరచడం.

జవాబు: సి) ఆన్‌లైన్ పరస్పర చర్యలలో తాదాత్మ్యం మరియు దయను ప్రోత్సహించడం.

ప్రశ్న 8: కింది వాటిలో సైబర్ బెదిరింపుకు ఉదాహరణ కాదు?

ఎ) అనుమతి లేకుండా ఒకరి ప్రైవేట్ సమాచారాన్ని పంచుకోవడం.

బి) ఆన్‌లైన్‌లో ఒకరిపై తప్పుడు పుకార్లు వ్యాప్తి చేయడం.

సి) గౌరవప్రదమైన రీతిలో నిర్మాణాత్మక విమర్శలను అందించడం.

డి) సోషల్ మీడియాలో ఎవరికైనా బెదిరింపు సందేశాలు పంపడం.

జవాబు: సి) గౌరవప్రదమైన రీతిలో నిర్మాణాత్మక విమర్శలను అందించడం.

ప్రశ్న 9: పిల్లలలో సైబర్ బెదిరింపులను నిరోధించడంలో తల్లిదండ్రులు మరియు విద్యావేత్తలు ఎలా సహాయపడగలరు?

ఎ) పిల్లలు సైబర్ బెదిరింపులను ఎదుర్కొన్నప్పుడు ప్రతీకారం తీర్చుకునేలా ప్రోత్సహించడం.

బి) ఇంటర్నెట్ మరియు డిజిటల్ పరికరాలకు పిల్లల ప్రాప్యతను పరిమితం చేయడం.

సి) బాధ్యతాయుతమైన ఆన్‌లైన్ ప్రవర్తన మరియు తాదాత్మ్యం గురించి పిల్లలకు బోధించడం.

డి) సైబర్ బెదిరింపులకు గురైనందుకు బాధితులను నిందించడం.

జవాబు: సి) బాధ్యతాయుతమైన ఆన్‌లైన్ ప్రవర్తన మరియు తాదాత్మ్యం గురించి పిల్లలకు బోధించడం.

ప్రశ్న 10: సైబర్ బెదిరింపు ఎవరికైనా జరుగుతున్నట్లు మీరు చూసినట్లయితే అత్యంత సరైన చర్య ఏమిటి?

ఎ) మీరే లక్ష్యంగా మారకుండా ఉండటానికి సైబర్ బెదిరింపులో చేరడం.

బి) పరిస్థితిని విస్మరించడం మరియు జోక్యం చేసుకోకపోవడం.

సి) సంఘటనను తగిన ప్లాట్‌ఫారమ్ లేదా అధికారానికి నివేదించడం.

డి) బాధితుడిని ఎదుర్కోవడం మరియు సైబర్ బెదిరింపుకు వారిని నిందించడం.

సమాధానం: సి) సంఘటనను తగిన ప్లాట్‌ఫారమ్ లేదా అధికారానికి నివేదించడం.

Day – 4

మొబైల్ భద్రత

ప్రశ్న 1:

మొబైల్ సెక్యూరిటీ అంటే ఏమిటి?

ఎ) భౌతిక మొబైల్ పరికరాన్ని దొంగతనం నుండి భద్రపరిచే ప్రక్రియ

బి) మొబైల్ యాప్‌లను అనధికార యాక్సెస్ నుండి రక్షించడం

సి) బెదిరింపులు మరియు దుర్బలత్వాల నుండి మొబైల్ పరికరాలు మరియు వాటి డేటా యొక్క భద్రత మరియు రక్షణను నిర్ధారించడం

D) అనధికారిక యాక్సెస్ నుండి మొబైల్ నెట్‌వర్క్ కనెక్షన్‌లను సురక్షితం చేయడం

జవాబు: సి) బెదిరింపులు మరియు దుర్బలత్వాల నుండి మొబైల్ పరికరాలు మరియు వాటి డేటా యొక్క భద్రత మరియు రక్షణను నిర్ధారించడం

ప్రశ్న 2:

కొన్ని సాధారణ మొబైల్ భద్రతా బెదిరింపులు ఏమిటి?

ఎ) మొబైల్ పరికరానికి భౌతిక నష్టం

బి) యాప్‌ల ఆకస్మిక తొలగింపు

సి) మొబైల్ పరికరాలను లక్ష్యంగా చేసుకునే మాల్వేర్ మరియు వైరస్లు

D) తరచుగా సాఫ్ట్‌వేర్ నవీకరణలు

సమాధానం: సి) మొబైల్ పరికరాలను లక్ష్యంగా చేసుకునే మాల్వేర్ మరియు వైరస్లు

ప్రశ్న 3:

మొబైల్ భద్రత విషయంలో "జైల్‌బ్రేకింగ్" లేదా "రూటింగ్" అంటే ఏమిటి?

ఎ) మొబైల్ పరికరానికి భౌతిక నష్టాన్ని సరిచేసే ప్రక్రియ

బి) పరికరం నుండి అవాంఛిత యాప్‌లను తీసివేయడానికి ఉపయోగించే సాంకేతికత

సి) అడ్మినిస్ట్రేటివ్ యాక్సెస్ పొందడానికి పరికరం యొక్క ఆపరేటింగ్ సిస్టమ్‌ను అన్‌లాక్ చేయడం

డి) పరికర తయారీదారు నుండి అధికారిక సాఫ్ట్‌వేర్ నవీకరణలను ఇన్‌స్టాల్ చేయడం

సమాధానం: సి) అడ్మినిస్ట్రేటివ్ యాక్సెస్ పొందడానికి పరికరం యొక్క ఆపరేటింగ్ సిస్టమ్‌ను అన్‌లాక్ చేయడం

ప్రశ్న 4:

మొబైల్ పరికరాలలో బలమైన మరియు ప్రత్యేకమైన పాస్‌వర్డ్‌లను ఉపయోగించడం ఎందుకు అవసరం?

ఎ) పాస్‌వర్డ్ సంక్లిష్టతతో ఇతరులను ఆకట్టుకోవడానికి

బి) ప్రమాదవశాత్తు డేటా నష్టాన్ని నిరోధించడానికి

సి) అతుకులు లేని సాఫ్ట్‌వేర్ నవీకరణలను నిర్ధారించడానికి

D) అనధికార యాక్సెస్ నుండి పరికరం మరియు దాని డేటాను రక్షించడానికి

సమాధానం: D) అనధికార యాక్సెస్ నుండి పరికరం మరియు దాని డేటాను రక్షించడానికి

ప్రశ్న 5:

మొబైల్ భద్రత విషయంలో "యాప్ అనుమతులు" అంటే ఏమిటి?

ఎ) పరికరం యొక్క హార్డ్‌వేర్‌ను సవరించడానికి నిర్దిష్ట యాప్‌లకు యాక్సెస్‌ను మంజూరు చేసే ప్రక్రియ

బి) పరికరం యొక్క హోమ్ స్క్రీన్ నుండి యాప్‌లను దాచే చర్య

సి) పరికరంలో ముందే ఇన్‌స్టాల్ చేసిన యాప్‌లను తొలగించగల సామర్థ్యం

డి) పరికరంలోని నిర్దిష్ట ఫీచర్‌లు మరియు డేటాను యాక్సెస్ చేయడానికి యాప్‌లు అభ్యర్థించిన అనుమతులు

సమాధానం: డి) పరికరంలోని నిర్దిష్ట ఫీచర్‌లు మరియు డేటాను యాక్సెస్ చేయడానికి యాప్‌లు అభ్యర్థించిన అనుమతులు

ప్రశ్న 6:

మీరు మీ మొబైల్ పరికరాన్ని మాల్వేర్ మరియు వైరస్‌ల నుండి ఎలా రక్షించుకోవచ్చు?

ఎ) మొబైల్ పరికరాల కోసం ప్రత్యేకంగా రూపొందించిన యాంటీవైరస్ సాఫ్ట్‌వేర్‌ను ఉపయోగించడం ద్వారా

బి) మొబైల్ యాప్‌ల వినియోగాన్ని పూర్తిగా నివారించడం ద్వారా

సి) పరికరంలో ఇంటర్నెట్ యాక్సెస్‌ను పరిమితం చేయడం ద్వారా

డి) పరికరం నుండి అన్ని థర్డ్-పార్టీ యాప్‌లను అన్‌ఇన్‌స్టాల్ చేయడం ద్వారా

జవాబు: ఎ) మొబైల్ పరికరాల కోసం ప్రత్యేకంగా రూపొందించిన యాంటీవైరస్ సాఫ్ట్‌వేర్‌ను ఉపయోగించడం ద్వారా

ప్రశ్న 7:

మొబైల్ ఆపరేటింగ్ సిస్టమ్ మరియు యాప్‌లను తాజాగా ఉంచడం ఎందుకు కీలకం?

ఎ) పరికరం యొక్క బ్యాటరీ జీవితాన్ని మెరుగుపరచడానికి

బి) ప్రమాదవశాత్తు డేటా నష్టాన్ని నివారించడానికి

సి) కొత్త ఫీచర్లు మరియు కార్యాచరణలను స్వీకరించడానికి

D) భద్రతా లోపాలు మరియు బగ్‌లను సరిచేయడానికి

సమాధానం: D) భద్రతా లోపాలు మరియు బగ్‌లను సరిచేయడానికి

ప్రశ్న 8:

మొబైల్ భద్రత విషయంలో "రిమోట్ వైప్" అంటే ఏమిటి?

ఎ) పరికరం నుండి యాప్‌లను రిమోట్‌గా తొలగించే చర్య

బి) పరికరాన్ని రిమోట్‌గా షట్ డౌన్ చేసే ప్రక్రియ

సి) నష్టం లేదా దొంగతనం విషయంలో పరికరం నుండి మొత్తం డేటాను రిమోట్‌గా తొలగించగల సామర్థ్యం

డి) పరికరం నుండి రిమోట్‌గా అవాంఛిత యాప్‌లను అన్‌ఇన్‌స్టాల్ చేసే చర్య

సమాధానం: సి) నష్టం లేదా దొంగతనం జరిగినప్పుడు పరికరం నుండి మొత్తం డేటాను రిమోట్‌గా తొలగించగల సామర్థ్యం

ప్రశ్న 9:

అనధికారిక యాక్సెస్ నుండి మీ మొబైల్ పరికరంలో సున్నితమైన డేటాను మీరు ఎలా రక్షించగలరు?

ఎ) మీ పరికరం యొక్క పాస్‌వర్డ్‌ను విశ్వసనీయ స్నేహితులు మరియు కుటుంబ సభ్యులతో పంచుకోవడం ద్వారా

B) PIN, నమూనా లేదా బయోమెట్రిక్ ప్రమాణీకరణ వంటి స్క్రీన్ లాక్ పద్ధతులను ప్రారంభించడం ద్వారా

సి) దొంగతనాన్ని అరికట్టడానికి పరికరాన్ని బహిరంగ ప్రదేశాల్లో ఉంచడం ద్వారా

డి) పరికరం యొక్క నిల్వను గుప్తీకరించడం ద్వారా

సమాధానం: బి) PIN, నమూనా లేదా బయోమెట్రిక్ ప్రమాణీకరణ వంటి స్క్రీన్ లాక్ పద్ధతులను ప్రారంభించడం ద్వారా

ప్రశ్న 10:

మీ మొబైల్ పరికరం పోయినా లేదా దొంగిలించబడినా మీరు ఏమి చేయాలి?

ఎ) పరికరాన్ని కనుగొన్న వ్యక్తి తిరిగి ఇచ్చే వరకు వేచి ఉండండి

బి) మీ మొబైల్ సర్వీస్ ప్రొవైడర్ మరియు పోలీసులకు నష్టం లేదా దొంగతనం గురించి వెంటనే నివేదించండి

సి) పరికరాన్ని తిరిగి ఇవ్వమని ఎవరైనా ప్రోత్సహించడానికి సోషల్ మీడియాలో రివార్డ్‌ను పోస్ట్ చేయండి

డి) పరికరం ప్రస్తుత స్థానాన్ని గుర్తించడానికి ట్రాకింగ్ యాప్‌ను ఇన్‌స్టాల్ చేయండి

సమాధానం: బి) మీ మొబైల్ సర్వీస్ ప్రొవైడర్ మరియు పోలీసులకు నష్టం లేదా దొంగతనం గురించి వెంటనే నివేదించండి

**సోషల్ నెట్వర్కింగ్**

ప్రశ్న 1:

సోషల్ నెట్‌వర్కింగ్ అంటే ఏమిటి?

ఎ) ఆన్‌లైన్ ప్లాట్‌ఫారమ్‌ల ద్వారా సంబంధాలను నిర్మించడం మరియు నిర్వహించడం

బి) లేఖల ద్వారా స్నేహితులు మరియు కుటుంబ సభ్యులతో వ్యక్తిగత అనుభవాలను పంచుకునే చర్య

సి) సోషల్ మీడియాలో వ్యాపారం మరియు వృత్తిపరమైన పరస్పర చర్యలను నిర్వహించడం

D) ఉత్పత్తులు మరియు సేవలను ప్రచారం చేయడానికి సోషల్ మీడియాను ఉపయోగించడం

జవాబు: ఎ) ఆన్‌లైన్ ప్లాట్‌ఫారమ్‌ల ద్వారా సంబంధాలను నిర్మించడం మరియు నిర్వహించడం

ప్రశ్న 2:

సోషల్ నెట్‌వర్కింగ్‌తో సంబంధం ఉన్న కొన్ని సంభావ్య హాని ఏమిటి?

ఎ) పెరిగిన సామాజిక పరస్పర చర్యలు మరియు బలమైన సంబంధాలు

బి) మానసిక ఆరోగ్యం మెరుగుపడుతుంది మరియు ఒత్తిడి తగ్గుతుంది

సి) సైబర్ బెదిరింపు, ఆన్‌లైన్ వేధింపు మరియు ప్రతికూల సామాజిక పోలిక

డి) ఆత్మగౌరవం మరియు విశ్వాసాన్ని పెంచడం

సమాధానం: సి) సైబర్ బెదిరింపు, ఆన్‌లైన్ వేధింపు మరియు ప్రతికూల సామాజిక పోలిక

ప్రశ్న 3:

సోషల్ నెట్‌వర్కింగ్ ప్లాట్‌ఫారమ్‌లలో వ్యక్తిగత సమాచారాన్ని పంచుకోవడంలో జాగ్రత్తగా ఉండటం ఎందుకు అవసరం?

ఎ) మీ ఆన్‌లైన్ కీర్తిని మరియు ఇమేజ్‌ని కాపాడుకోవడానికి

బి) ఎక్కువ మంది అనుచరులు మరియు ప్రజాదరణ పొందడం

సి) మీ పోస్ట్‌లపై మరిన్ని లైక్‌లు మరియు కామెంట్‌లను స్వీకరించడానికి

D) కొత్త స్నేహితులను మరియు కనెక్షన్‌లను సంపాదించడానికి

సమాధానం: ఎ) మీ ఆన్‌లైన్ కీర్తి మరియు ఇమేజ్‌ని రక్షించడానికి

ప్రశ్న 4:

సోషల్ నెట్‌వర్కింగ్ సందర్భంలో "సైబర్ బెదిరింపు" అంటే ఏమిటి?

ఎ) ఆన్‌లైన్ స్నేహితులతో స్నేహపూర్వక పరిహాసాలు మరియు జోకులలో పాల్గొనడం

బి) ఆన్‌లైన్ సంఘర్షణలలో మీ స్నేహితులకు మద్దతు ఇవ్వడం మరియు రక్షించడం

సి) ఇతరులను వేధించడానికి, భయపెట్టడానికి లేదా అవమానించడానికి ఎలక్ట్రానిక్ కమ్యూనికేషన్‌ను ఉపయోగించే చర్య

డి) సోషల్ మీడియాలో సానుకూల మరియు ప్రేరణాత్మక కంటెంట్‌ను సృష్టించడం మరియు భాగస్వామ్యం చేయడం

జవాబు: సి) ఇతరులను వేధించడానికి, భయపెట్టడానికి లేదా అవమానించడానికి ఎలక్ట్రానిక్ కమ్యూనికేషన్‌ను ఉపయోగించే చర్య

ప్రశ్న 5:

సోషల్ నెట్‌వర్కింగ్ ప్లాట్‌ఫారమ్‌ల అధిక వినియోగం మానసిక ఆరోగ్యాన్ని ఎలా ప్రతికూలంగా ప్రభావితం చేస్తుంది?

ఎ) సానుకూల సామాజిక పరస్పర చర్యలను ప్రోత్సహించడం మరియు ఒంటరితనాన్ని తగ్గించడం ద్వారా

బి) సానుకూల అభిప్రాయం ద్వారా ఆత్మగౌరవం మరియు స్వీయ-విలువను పెంపొందించడం ద్వారా

సి) సోషల్ మీడియా వ్యసనం మరియు ఆందోళన, నిరాశ మరియు ఒంటరితనం యొక్క భావాలకు దారితీయడం ద్వారా

డి) మొత్తం శ్రేయస్సు మరియు జీవిత సంతృప్తిని మెరుగుపరచడం ద్వారా

సమాధానం: సి) సోషల్ మీడియా వ్యసనం మరియు ఆందోళన, నిరాశ మరియు ఒంటరితనం యొక్క భావాలకు దారితీయడం ద్వారా

ప్రశ్న 6:

సోషల్ నెట్‌వర్కింగ్ సందర్భంలో "ఆన్‌లైన్ వేధింపు" అంటే ఏమిటి?

ఎ) ఆన్‌లైన్‌లో ఇతరులతో సహాయకరమైన సమాచారం మరియు వనరులను పంచుకునే చర్య

బి) సానుకూల సందేశాలు మరియు న్యాయవాదాన్ని ప్రోత్సహించడానికి సోషల్ మీడియాను ఉపయోగించే ప్రక్రియ

సి) ఆన్‌లైన్ కమ్యూనికేషన్ ద్వారా వ్యక్తులను లక్ష్యంగా చేసుకోవడం మరియు భయపెట్టడం

డి) సోషల్ మీడియాలో స్నేహపూర్వక చర్చలు మరియు చర్చలలో పాల్గొనడం

జవాబు: సి) ఆన్‌లైన్ కమ్యూనికేషన్ ద్వారా వ్యక్తులను లక్ష్యంగా చేసుకోవడం మరియు భయపెట్టడం

ప్రశ్న 7:

ప్రతికూల సామాజిక పోలికకు సోషల్ నెట్‌వర్కింగ్ ప్లాట్‌ఫారమ్‌లు ఎలా దోహదపడతాయి?

ఎ) వినియోగదారులు తమ సొంత బలాలు మరియు విజయాలపై దృష్టి పెట్టేలా ప్రోత్సహించడం ద్వారా

బి) వినియోగదారులకు ఇతరుల కష్టాలతో కనెక్ట్ అయ్యేందుకు మరియు సానుభూతి పొందేందుకు వేదికను అందించడం ద్వారా

సి) వినియోగదారుల జీవితాల యొక్క క్యూరేటెడ్ మరియు ఆదర్శవంతమైన సంస్కరణలను ప్రదర్శించడం ద్వారా, పోల్చి చూస్తే సరిపోని భావాలకు దారి తీస్తుంది

D) వినియోగదారుల నుండి ప్రామాణికమైన మరియు ఫిల్టర్ చేయని కంటెంట్‌ను ప్రచారం చేయడం ద్వారా

సమాధానం: సి) వినియోగదారుల జీవితాల యొక్క క్యూరేటెడ్ మరియు ఆదర్శవంతమైన సంస్కరణలను ప్రదర్శించడం ద్వారా, పోల్చి చూస్తే సరిపోని భావాలకు దారి తీస్తుంది

ప్రశ్న 8:

సోషల్ నెట్‌వర్కింగ్ ప్లాట్‌ఫారమ్‌లలో "ఓవర్‌షేరింగ్" అంటే ఏమిటి?

ఎ) సానుకూల మరియు ఉత్తేజకరమైన కంటెంట్‌ను క్రమం తప్పకుండా పంచుకునే చర్య

బి) వ్యక్తిగత సమాచారం, అనుభవాలు లేదా అభిప్రాయాలను అతిగా మరియు జాగ్రత్త లేకుండా పంచుకోవడం

సి) సోషల్ మీడియాలో అనుచరుల సంఖ్య మరియు కనెక్షన్‌లను పరిమితం చేయడం

D) సోషల్ మీడియాలో ఇతరులతో సానుకూల మరియు సహాయక పరస్పర చర్యలలో పాల్గొనడం

జవాబు: బి) వ్యక్తిగత సమాచారం, అనుభవాలు లేదా అభిప్రాయాలను అతిగా మరియు జాగ్రత్త లేకుండా పంచుకోవడం

ప్రశ్న 9:

సోషల్ నెట్‌వర్కింగ్ హాని నుండి మిమ్మల్ని మీరు ఎలా రక్షించుకోవచ్చు?

ఎ) బలమైన కనెక్షన్‌లను నిర్మించడానికి సోషల్ మీడియాలో ఎక్కువ సమయం గడపడం ద్వారా

బి) ఆన్‌లైన్ స్నేహితులతో ఉచితంగా వ్యక్తిగత సమాచారం మరియు అనుభవాలను పంచుకోవడం ద్వారా

సి) గోప్యతా సెట్టింగ్‌లను సెట్ చేయడం ద్వారా మరియు మీరు భాగస్వామ్యం చేసే కంటెంట్ గురించి జాగ్రత్తగా ఉండటం ద్వారా

డి) సోషల్ నెట్‌వర్కింగ్ ప్లాట్‌ఫారమ్‌లను పూర్తిగా నివారించడం ద్వారా

సమాధానం: సి) గోప్యతా సెట్టింగ్‌లను సెట్ చేయడం ద్వారా మరియు మీరు భాగస్వామ్యం చేసే కంటెంట్ గురించి జాగ్రత్తగా ఉండటం ద్వారా

ప్రశ్న 10:

మీరు సోషల్ నెట్‌వర్కింగ్ ప్లాట్‌ఫారమ్‌లలో సైబర్ బెదిరింపు లేదా ఆన్‌లైన్ వేధింపులను ఎదుర్కొంటే మీరు ఏమి చేయాలి?

ఎ) నేరస్థులతో ఘర్షణలు మరియు వాదనలలో పాల్గొనండి

బి) ప్లాట్‌ఫారమ్ నిర్వాహకులు లేదా మోడరేటర్‌లకు సంఘటనలను నివేదించండి

సి) మద్దతు కోసం సంఘటనలను స్నేహితులు మరియు కుటుంబ సభ్యులతో పంచుకోండి

డి) వేధింపులను విస్మరించండి మరియు అది దానంతటదే ఆగిపోతుందని ఆశిస్తున్నాము

సమాధానం: బి) ప్లాట్‌ఫారమ్ నిర్వాహకులు లేదా మోడరేటర్‌లకు సంఘటనలను నివేదించండి

నకిలీ అప్లికేషన్స్ గుర్తించడం ఎలా

ప్రశ్న 1:

నకిలీ అప్లికేషన్లు ఏమిటి?

ఎ) పేరున్న కంపెనీలు అభివృద్ధి చేసిన చట్టబద్ధమైన మొబైల్ యాప్‌లు

బి) వినియోగదారులకు తగ్గింపులు మరియు ప్రమోషన్‌లను అందించే అప్లికేషన్‌లు

సి) వినియోగదారులను మోసం చేయడానికి లేదా సున్నితమైన సమాచారాన్ని దొంగిలించడానికి రూపొందించబడిన హానికరమైన యాప్‌లు

D) పరిమిత కార్యాచరణ మరియు లక్షణాలను అందించే యాప్‌లు

సమాధానం: సి) వినియోగదారులను మోసం చేయడానికి లేదా సున్నితమైన సమాచారాన్ని దొంగిలించడానికి రూపొందించబడిన హానికరమైన యాప్‌లు

ప్రశ్న 2:

నకిలీ అప్లికేషన్‌లను పంపిణీ చేసే సాధారణ మార్గం ఏమిటి?

A) Google Play మరియు Apple App Store వంటి అధికారిక యాప్ స్టోర్‌ల ద్వారా

బి) సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లలో డైరెక్ట్ లింక్‌లను షేర్ చేయడం ద్వారా

సి) తెలియని మూలాల నుండి ఇమెయిల్ జోడింపుల ద్వారా

D) అప్లికేషన్ యొక్క భౌతిక కాపీలను వినియోగదారులకు పంపడం ద్వారా

సమాధానం: బి) సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లలో డైరెక్ట్ లింక్‌లను షేర్ చేయడం ద్వారా

ప్రశ్న 3:

మీరు మొబైల్ అప్లికేషన్‌ను డౌన్‌లోడ్ చేసే ముందు దాని చట్టబద్ధతను ఎలా తనిఖీ చేయవచ్చు?

ఎ) యాప్ స్టోర్‌లలో ఇతర వినియోగదారుల నుండి సమీక్షలు మరియు రేటింగ్‌లను చదవండి

బి) ఒక ప్రసిద్ధ సంస్థ నుండి క్లెయిమ్ చేసే ఏదైనా అప్లికేషన్‌ను విశ్వసించండి

సి) ప్రత్యేకమైన కంటెంట్‌ను యాక్సెస్ చేయడానికి అనధికారిక యాప్ స్టోర్‌ల నుండి అప్లికేషన్‌లను డౌన్‌లోడ్ చేయండి

D) సొగసైన గ్రాఫిక్స్ మరియు డిజైన్‌లతో వెబ్‌సైట్‌ల నుండి మాత్రమే అప్లికేషన్‌లను డౌన్‌లోడ్ చేయండి

సమాధానం: ఎ) యాప్ స్టోర్‌లలో ఇతర వినియోగదారుల నుండి సమీక్షలు మరియు రేటింగ్‌లను చదవండి

ప్రశ్న 4:

ఇన్‌స్టాలేషన్ సమయంలో మొబైల్ అప్లికేషన్ అధిక అనుమతులను అభ్యర్థించినప్పుడు మీరు ఏమి జాగ్రత్త వహించాలి?

ఎ) చట్టబద్ధమైన యాప్‌లు మెరుగైన కార్యాచరణ కోసం అనేక అనుమతులను అభ్యర్థించడం సాధారణం

బి) అధిక అనుమతులు మెరుగైన వినియోగదారు అనుభవానికి దారి తీయవచ్చు

సి) అధిక అనుమతులు మంజూరు చేయడం వలన మీ గోప్యత మరియు భద్రతకు హాని కలుగవచ్చు

D) వినియోగదారు ప్రవర్తనను ట్రాక్ చేయడానికి యాప్ డెవలపర్‌లకు అధిక అనుమతులు అవసరం

సమాధానం: సి) మితిమీరిన అనుమతులు మంజూరు చేయడం వలన మీ గోప్యత మరియు భద్రతకు హాని కలుగవచ్చు

ప్రశ్న 5:

నకిలీ అప్లికేషన్ యొక్క కొన్ని హెచ్చరిక సంకేతాలు ఏమిటి?

ఎ) యాప్ స్టోర్‌లలో తక్కువ రేటింగ్‌లు మరియు ప్రతికూల సమీక్షలు

బి) ఆకర్షించే చిహ్నాలు మరియు దృశ్యమానంగా ఆకట్టుకునే డిజైన్‌లు

సి) ఇన్‌స్టాలేషన్ తర్వాత ఉచిత బహుమతులు మరియు రివార్డుల వాగ్దానాలు

డి) సోషల్ మీడియా ప్రభావితం చేసేవారి నుండి ధృవీకరించబడిన బ్యాడ్జ్‌లు మరియు ఎండార్స్‌మెంట్‌లు

సమాధానం: ఎ) యాప్ స్టోర్‌లలో తక్కువ రేటింగ్‌లు మరియు ప్రతికూల సమీక్షలు

ప్రశ్న 6:

అప్లికేషన్‌ను డౌన్‌లోడ్ చేయడానికి ముందు యాప్ డెవలపర్ లేదా ప్రచురణకర్త యొక్క చట్టబద్ధతను ధృవీకరించడం ఎందుకు కీలకం?

ఎ) చట్టబద్ధమైన డెవలపర్‌లు ఎల్లప్పుడూ వారి పూర్తి సంప్రదింపు సమాచారాన్ని యాప్ పేజీలో కలిగి ఉంటారు

బి) యాప్‌లను డౌన్‌లోడ్ చేసే విషయంలో డెవలపర్ గుర్తింపు ముఖ్యం కాదు

సి) నకిలీ డెవలపర్లు తమ నిజమైన ఉద్దేశాలను దాచడానికి తరచుగా సాధారణ లేదా అనుమానాస్పద పేర్లను ఉపయోగిస్తారు

డి) ధృవీకరించబడిన డెవలపర్‌లు వారి యాప్‌లకు మెరుగైన కస్టమర్ మద్దతును అందిస్తారు

సమాధానం: సి) నకిలీ డెవలపర్లు తమ నిజమైన ఉద్దేశాలను దాచడానికి తరచుగా సాధారణ లేదా అనుమానాస్పద పేర్లను ఉపయోగిస్తారు

ప్రశ్న 7:

మీరు నకిలీ అప్లికేషన్‌ను ఎదుర్కొంటే లేదా యాప్ హానికరమైనదిగా అనుమానించినట్లయితే మీరు ఏమి చేయాలి?

ఎ) వారి అభిప్రాయాలను సేకరించడానికి స్నేహితులు మరియు కుటుంబ సభ్యులతో యాప్‌ను భాగస్వామ్యం చేయండి

బి) ఏమైనప్పటికీ యాప్‌ని డౌన్‌లోడ్ చేసి, మీ పరికరంలో పరీక్షించండి

సి) యాప్‌ను అధికారిక యాప్ స్టోర్‌కు నివేదించి, మీ పరికరం నుండి తొలగించండి

D) నకిలీ యాప్ గురించి ఇతరులను హెచ్చరించడానికి యాప్ స్టోర్‌లో సానుకూల సమీక్షను ఇవ్వండి

సమాధానం: సి) యాప్‌ను అధికారిక యాప్ స్టోర్‌కు నివేదించి, మీ పరికరం నుండి తొలగించండి

ప్రశ్న 8:

పాస్‌వర్డ్‌లు లేదా క్రెడిట్ కార్డ్ వివరాల వంటి సున్నితమైన సమాచారాన్ని అభ్యర్థిస్తున్న నకిలీ అప్లికేషన్‌ల ప్రయోజనం ఏమిటి?

ఎ) యాప్ యొక్క కార్యాచరణ మరియు వినియోగదారు అనుభవాన్ని మెరుగుపరచడానికి

బి) చట్టబద్ధమైన లావాదేవీల ద్వారా డబ్బు సంపాదించడం

సి) వినియోగదారు భద్రతను రాజీ చేయడం మరియు సున్నితమైన సమాచారాన్ని దొంగిలించడం

D) వినియోగదారులకు వ్యక్తిగతీకరించిన కంటెంట్ మరియు సిఫార్సులను అందించడానికి

సమాధానం: సి) యూజర్ యొక్క భద్రతను రాజీ చేయడానికి మరియు సున్నితమైన సమాచారాన్ని దొంగిలించడానికి

ప్రశ్న 9:

మీ మొబైల్ పరికరం యొక్క ఆపరేటింగ్ సిస్టమ్ మరియు అప్లికేషన్‌లను తాజాగా ఉంచడం ఎందుకు అవసరం?

ఎ) నకిలీ అప్లికేషన్ల ఇన్‌స్టాలేషన్‌ను నిరోధించడానికి

బి) తాజా యాప్ ఫీచర్‌లు మరియు ఫంక్షనాలిటీలను యాక్సెస్ చేయడానికి

సి) పరికరం పనితీరు మరియు బ్యాటరీ జీవితాన్ని మెరుగుపరచడానికి

D) దుర్బలత్వాల నుండి రక్షించే భద్రతా పాచెస్ మరియు బగ్ పరిష్కారాలను స్వీకరించడానికి

సమాధానం: D) దుర్బలత్వాల నుండి రక్షించే భద్రతా ప్యాచ్‌లు మరియు బగ్ పరిష్కారాలను స్వీకరించడానికి

ప్రశ్న 10:

నకిలీ అప్లికేషన్‌లను డౌన్‌లోడ్ చేయకుండా ఉండటానికి మీరు ఏమి చేయాలి?

ఎ) ధృవీకరించబడిన యాప్ స్టోర్‌లు మరియు అధికారిక వెబ్‌సైట్‌ల నుండి మాత్రమే అప్లికేషన్‌లను డౌన్‌లోడ్ చేయండి

బి) ఉచిత కంటెంట్‌ను అందించే ఏదైనా వెబ్‌సైట్ నుండి అప్లికేషన్‌లను డౌన్‌లోడ్ చేయండి

సి) మెరుగైన యాప్ సిఫార్సుల కోసం యాప్ డెవలపర్‌లతో మీ వ్యక్తిగత సమాచారాన్ని ఉచితంగా షేర్ చేయండి

డి) అనేక రకాల అప్లికేషన్‌లను యాక్సెస్ చేయడానికి మీ పరికరంలో బహుళ యాప్ స్టోర్‌లను ఇన్‌స్టాల్ చేయండి

సమాధానం: ఎ) ధృవీకరించబడిన యాప్ స్టోర్‌లు మరియు అధికారిక వెబ్‌సైట్‌ల నుండి మాత్రమే అప్లికేషన్‌లను డౌన్‌లోడ్ చేసుకోండి

**డెస్క్‌టాప్ భద్రత**

ప్రశ్న 1:

డెస్క్‌టాప్ భద్రత అంటే ఏమిటి?

ఎ) డెస్క్‌టాప్ కంప్యూటర్ యొక్క భౌతిక భాగాలను భద్రపరిచే అభ్యాసం

బి) అనధికార మార్పుల నుండి డెస్క్‌టాప్ వాల్‌పేపర్‌ను రక్షించడం

సి) డెస్క్‌టాప్ కంప్యూటర్‌లు మరియు వాటి డేటా యొక్క భద్రత మరియు రక్షణను బెదిరింపులు మరియు దుర్బలత్వాల నుండి నిర్ధారించడం

D) అదనపు హార్డ్‌వేర్ భాగాలను ఇన్‌స్టాల్ చేయడం ద్వారా డెస్క్‌టాప్ కంప్యూటర్‌ల పనితీరును మెరుగుపరచడం

జవాబు: సి) డెస్క్‌టాప్ కంప్యూటర్‌ల భద్రత మరియు రక్షణ మరియు వాటి డేటా బెదిరింపులు మరియు దుర్బలత్వాల నుండి భరోసా

ప్రశ్న 2:

డెస్క్‌టాప్ కంప్యూటర్‌లకు కొన్ని సంభావ్య భద్రతా బెదిరింపులు ఏమిటి?

ఎ) కంప్యూటర్ కేస్ లోపల దుమ్ము మరియు చెత్త పేరుకుపోవడం

బి) డెస్క్‌టాప్ అప్లికేషన్‌లు మరియు సాఫ్ట్‌వేర్‌ల అధిక వినియోగం

సి) డెస్క్‌టాప్ సిస్టమ్‌లను లక్ష్యంగా చేసుకుని మాల్వేర్, వైరస్‌లు మరియు సైబర్‌టాక్‌లు

D) చట్టబద్ధమైన విక్రేతల నుండి తరచుగా సాఫ్ట్‌వేర్ నవీకరణలు

జవాబు: సి) డెస్క్‌టాప్ సిస్టమ్‌లను లక్ష్యంగా చేసుకుని మాల్వేర్, వైరస్‌లు మరియు సైబర్‌టాక్‌లు

ప్రశ్న 3:

డెస్క్‌టాప్ ఖాతాల కోసం బలమైన మరియు ప్రత్యేకమైన పాస్‌వర్డ్‌లను ఉపయోగించడం ఎందుకు ముఖ్యం?

ఎ) పాస్‌వర్డ్‌లను గుర్తుంచుకోవడం మరింత కష్టతరం చేయడానికి

బి) డెస్క్‌టాప్ మరియు సెన్సిటివ్ డేటాకు అనధికారిక యాక్సెస్‌ను నిరోధించడానికి

సి) డెస్క్‌టాప్ హార్డ్‌వేర్ భాగాల పనితీరును మెరుగుపరచడానికి

D) సాఫ్ట్‌వేర్ విక్రేతల నుండి తగ్గింపులు మరియు ప్రమోషన్‌లను స్వీకరించడానికి

సమాధానం: బి) డెస్క్‌టాప్ మరియు సున్నితమైన డేటాకు అనధికారిక యాక్సెస్‌ను నిరోధించడానికి

ప్రశ్న 4:

డెస్క్‌టాప్ భద్రత విషయంలో "ఫైర్‌వాల్" అంటే ఏమిటి?

ఎ) భౌతిక బెదిరింపుల నుండి డెస్క్‌టాప్ కంప్యూటర్‌ను రక్షించడానికి భౌతిక అవరోధం

బి) నెట్‌వర్క్ ట్రాఫిక్‌ను పర్యవేక్షించడానికి మరియు నియంత్రించడానికి సాఫ్ట్‌వేర్ లేదా హార్డ్‌వేర్ సెక్యూరిటీ మెకానిజం

సి) గీతలు పడకుండా డెస్క్‌టాప్ మానిటర్‌కు రక్షణ కవచం

D) డెస్క్‌టాప్ అప్లికేషన్‌లు మరియు సాఫ్ట్‌వేర్‌లను ఆటోమేటిక్‌గా అప్‌డేట్ చేసే ఫీచర్

జవాబు: బి) నెట్‌వర్క్ ట్రాఫిక్‌ను పర్యవేక్షించడానికి మరియు నియంత్రించడానికి సాఫ్ట్‌వేర్ లేదా హార్డ్‌వేర్ సెక్యూరిటీ మెకానిజం

ప్రశ్న 5:

మీరు మీ డెస్క్‌టాప్ కంప్యూటర్‌ను మాల్వేర్ మరియు వైరస్‌ల నుండి ఎలా రక్షించుకోవచ్చు?

ఎ) ఇంటర్నెట్ కనెక్టివిటీ మరియు ఆన్‌లైన్ కార్యకలాపాలను నివారించడం ద్వారా

బి) నమ్మదగిన యాంటీవైరస్ మరియు యాంటీ మాల్వేర్ సాఫ్ట్‌వేర్‌ను ఇన్‌స్టాల్ చేయడం ద్వారా

సి) కాలం చెల్లిన మరియు మద్దతు లేని ఆపరేటింగ్ సిస్టమ్‌లు మరియు అప్లికేషన్‌లను ఉపయోగించడం ద్వారా

D) మీ డెస్క్‌టాప్ భద్రతా వివరాలను స్నేహితులు మరియు కుటుంబ సభ్యులతో పంచుకోవడం ద్వారా

సమాధానం: బి) నమ్మకమైన యాంటీవైరస్ మరియు యాంటీ మాల్వేర్ సాఫ్ట్‌వేర్‌ను ఇన్‌స్టాల్ చేయడం ద్వారా

ప్రశ్న 6:

డెస్క్‌టాప్ భద్రత విషయంలో "ఫిషింగ్" అంటే ఏమిటి?

ఎ) డెస్క్‌టాప్ స్క్రీన్ యొక్క ఇమేజ్‌లు లేదా స్క్రీన్‌షాట్‌లను క్యాప్చర్ చేసే చర్య

బి) డెస్క్‌టాప్ హార్డ్‌వేర్ భాగాలకు సంబంధించిన సమాచారం కోసం ఫిషింగ్ ప్రక్రియ

సి) సున్నితమైన సమాచారాన్ని బహిర్గతం చేయడానికి వినియోగదారులను మోసగించడానికి ఇమెయిల్‌లు లేదా సందేశాలను ఉపయోగించే చర్య

D) నకిలీ డెస్క్‌టాప్ థీమ్‌లు మరియు వాల్‌పేపర్‌లను ఇన్‌స్టాల్ చేసే పద్ధతి

సమాధానం: సి) సున్నితమైన సమాచారాన్ని బహిర్గతం చేయడానికి వినియోగదారులను మోసగించడానికి ఇమెయిల్‌లు లేదా సందేశాలను ఉపయోగించే చర్య

ప్రశ్న 7:

డెస్క్‌టాప్ సాఫ్ట్‌వేర్ మరియు ఆపరేటింగ్ సిస్టమ్‌లను తాజాగా ఉంచడం ఎందుకు కీలకం?

ఎ) డెస్క్‌టాప్ ఇంటర్‌ఫేస్ యొక్క దృశ్య రూపాన్ని మరియు సౌందర్యాన్ని మెరుగుపరచడానికి

బి) డెస్క్‌టాప్ అప్లికేషన్‌లు ఎలాంటి సమస్యలు లేకుండా సాఫీగా రన్ అయ్యేలా చూసుకోవడానికి

సి) దుర్బలత్వాల నుండి రక్షించే తాజా భద్రతా ప్యాచ్‌లు మరియు బగ్ పరిష్కారాలను స్వీకరించడానికి

D) డెస్క్‌టాప్‌ను యాక్సెస్ చేయకుండా అనధికార వినియోగదారులను నిరోధించడానికి

సమాధానం: సి) దుర్బలత్వాల నుండి రక్షించే తాజా భద్రతా ప్యాచ్‌లు మరియు బగ్ పరిష్కారాలను స్వీకరించడానికి

ప్రశ్న 8:

డెస్క్‌టాప్ భద్రత విషయంలో "టూ-ఫాక్టర్ అథెంటికేషన్" (2FA) అంటే ఏమిటి?

ఎ) ఫిజికల్ లాక్‌లతో డెస్క్‌టాప్ హార్డ్‌వేర్ భాగాలను భద్రపరిచే ప్రక్రియ

బి) అదనపు రక్షణ కోసం డెస్క్‌టాప్‌పై రెండు వేర్వేరు యాంటీవైరస్ సాఫ్ట్‌వేర్‌లను ఉపయోగించే చర్య

సి) వినియోగదారులు తమ ఖాతాలను యాక్సెస్ చేయడానికి రెండు రకాల గుర్తింపులను అందించాల్సిన భద్రతా ఫీచర్

D) డెస్క్‌టాప్ వాల్‌పేపర్‌లు మరియు స్క్రీన్‌సేవర్‌లను క్రమం తప్పకుండా అప్‌డేట్ చేసే అభ్యాసం

జవాబు: సి) వినియోగదారులు తమ ఖాతాలను యాక్సెస్ చేయడానికి రెండు రకాల గుర్తింపులను అందించాల్సిన భద్రతా ఫీచర్

ప్రశ్న 9:

ransomware వంటి డెస్క్‌టాప్ భద్రతా బెదిరింపుల బారిన పడకుండా మీరు ఎలా నివారించవచ్చు?

ఎ) ఇంటర్నెట్ కనెక్టివిటీ కోసం అసురక్షిత Wi-Fi నెట్‌వర్క్‌లను ఉపయోగించడం ద్వారా

B) బాహ్య నిల్వ పరికరానికి ముఖ్యమైన ఫైల్‌లు మరియు డేటాను క్రమం తప్పకుండా బ్యాకప్ చేయడం ద్వారా

సి) డెస్క్‌టాప్ పనితీరును మెరుగుపరచడానికి యాంటీవైరస్ సాఫ్ట్‌వేర్‌ను నిలిపివేయడం ద్వారా

డి) ఆన్‌లైన్‌లో తెలియని వ్యక్తులతో సున్నితమైన సమాచారాన్ని పంచుకోవడం ద్వారా

సమాధానం: B) బాహ్య నిల్వ పరికరానికి ముఖ్యమైన ఫైల్‌లు మరియు డేటాను క్రమం తప్పకుండా బ్యాకప్ చేయడం ద్వారా

ప్రశ్న 10:

మీ డెస్క్‌టాప్ కంప్యూటర్‌కు మాల్వేర్ సోకినట్లు మీరు అనుమానించినట్లయితే మీరు ఏమి చేయాలి?

ఎ) స్నేహితుల నుండి సలహా తీసుకోవడానికి సోషల్ మీడియాలో మీ ఆందోళనలను పంచుకోండి

బి) సంభావ్య సంక్రమణను విస్మరించండి ఎందుకంటే అది స్వయంగా పరిష్కరించవచ్చు

సి) యాంటీవైరస్ సాఫ్ట్‌వేర్‌ని ఉపయోగించి పూర్తి సిస్టమ్ స్కాన్‌ను అమలు చేయండి మరియు తగిన చర్య తీసుకోండి

D) సహాయం కోసం యాదృచ్ఛిక సాఫ్ట్‌వేర్ విక్రేత యొక్క కస్టమర్ మద్దతును సంప్రదించండి

సమాధానం: సి) యాంటీవైరస్ సాఫ్ట్‌వేర్‌ని ఉపయోగించి పూర్తి సిస్టమ్ స్కాన్‌ను అమలు చేయండి మరియు తగిన చర్య తీసుకోండి

**భద్రతా అవగాహన**

ప్రశ్న 1:

ధరించగలిగే గాడ్జెట్‌లు అంటే ఏమిటి?

ఎ) ఫ్యాషన్ ఉపకరణాలుగా ధరించడానికి ప్రత్యేకంగా రూపొందించిన పరికరాలు

బి) శారీరక దృఢత్వం మరియు ఆరోగ్య పర్యవేక్షణను పెంచే పరికరాలు

సి) వ్యాయామం చేసేటప్పుడు లేదా బహిరంగ కార్యకలాపాల్లో పాల్గొనేటప్పుడు మాత్రమే ఉపయోగించే గాడ్జెట్‌లు

డి) వినోదం మరియు గేమింగ్ ఫీచర్‌లను అందించే పరికరాలు

జవాబు: బి) శారీరక దృఢత్వం మరియు ఆరోగ్య పర్యవేక్షణను పెంచే పరికరాలు

ప్రశ్న 2:

ధరించగలిగే గాడ్జెట్‌లకు భద్రతా అవగాహన ఎందుకు ముఖ్యం?

ఎ) ధరించగలిగే గాడ్జెట్‌లు ఖరీదైనవి మరియు దొంగతనం నుండి రక్షించబడాలి

B) ధరించగలిగిన గాడ్జెట్‌లు భౌతిక నష్టానికి గురయ్యే అవకాశం ఉంది మరియు జాగ్రత్తగా నిర్వహించాల్సిన అవసరం ఉంది

సి) ధరించగలిగే గాడ్జెట్‌లు తరచుగా రక్షణ అవసరమయ్యే సున్నితమైన వ్యక్తిగత మరియు ఆరోగ్య డేటాను కలిగి ఉంటాయి

D) ధరించగలిగే గాడ్జెట్‌లు వేడెక్కడానికి అవకాశం ఉంది మరియు స్థిరమైన పర్యవేక్షణ అవసరం

సమాధానం: సి) ధరించగలిగే గాడ్జెట్‌లు తరచుగా రక్షణ అవసరమయ్యే సున్నితమైన వ్యక్తిగత మరియు ఆరోగ్య డేటాను కలిగి ఉంటాయి

ప్రశ్న 3:

ధరించగలిగే గాడ్జెట్‌లలో ఏ రకమైన వ్యక్తిగత సమాచారం నిల్వ చేయబడవచ్చు?

ఎ) చెల్లింపు కార్డ్ సమాచారం మరియు ఆర్థిక డేటా

బి) హృదయ స్పందన రేటు మరియు నిద్ర విధానాలు వంటి వ్యక్తిగత ఆరోగ్య డేటా

సి) సోషల్ మీడియా లాగిన్ ఆధారాలు మరియు ఇమెయిల్ పాస్‌వర్డ్‌లు

D) ఉపాధి మరియు ఉద్యోగ సంబంధిత సమాచారం

సమాధానం: బి) హృదయ స్పందన రేటు మరియు నిద్ర విధానాలు వంటి వ్యక్తిగత ఆరోగ్య డేటా

ప్రశ్న 4:

ధరించగలిగే గాడ్జెట్‌లతో సంబంధం ఉన్న కొన్ని సంభావ్య భద్రతా ప్రమాదాలు ఏమిటి?

ఎ) ఇతర పరికరాలతో కనెక్టివిటీ కోల్పోవడం

బి) దుస్తులు మరియు కన్నీటి కారణంగా భౌతిక నష్టం

సి) వ్యక్తిగత ఆరోగ్య డేటాకు అనధికారిక యాక్సెస్

D) పొడిగించిన ఉపయోగంలో వేడెక్కడం

సమాధానం: సి) వ్యక్తిగత ఆరోగ్య డేటాకు అనధికారిక యాక్సెస్

ప్రశ్న 5:

మీ ధరించగలిగే గాడ్జెట్ దొంగిలించబడినా లేదా పోగొట్టుకున్నా మీరు ఏమి చేయాలి?

ఎ) గాడ్జెట్ తయారీదారుకు నష్టాన్ని నివేదించండి

బి) పరికరం ట్రాకింగ్ లేదా రిమోట్ వైప్ ఫీచర్ అందుబాటులో ఉంటే యాక్టివేట్ చేయండి

సి) ధరించగలిగే గాడ్జెట్‌లు సున్నితమైన సమాచారాన్ని నిల్వ చేయనందున నష్టాన్ని విస్మరించండి

D) రిటర్న్‌ని ప్రోత్సహించడానికి సోషల్ మీడియాలో రివార్డ్‌ను పోస్ట్ చేయండి

సమాధానం: బి) అందుబాటులో ఉంటే పరికరం యొక్క ట్రాకింగ్ లేదా రిమోట్ వైప్ ఫీచర్‌ని యాక్టివేట్ చేయండి

ప్రశ్న 6:

ధరించగలిగే గాడ్జెట్ సాఫ్ట్‌వేర్‌ను తాజాగా ఉంచడం ఎందుకు ముఖ్యం?

ఎ) గాడ్జెట్ రూపాన్ని మరియు సౌందర్యాన్ని మెరుగుపరచడానికి

బి) గాడ్జెట్ అన్ని రకాల స్మార్ట్‌ఫోన్‌లకు అనుకూలంగా ఉండేలా చూసుకోవడం

సి) దుర్బలత్వాల నుండి రక్షించే భద్రతా నవీకరణలు మరియు బగ్ పరిష్కారాలను స్వీకరించడానికి

D) ధరించగలిగే గాడ్జెట్ యొక్క బ్యాటరీ జీవితాన్ని పెంచడానికి

జవాబు: సి) భద్రతా అప్‌డేట్‌లు మరియు దుర్బలత్వాల నుండి రక్షించే బగ్ పరిష్కారాలను స్వీకరించడానికి

ప్రశ్న 7:

అనధికారిక యాక్సెస్ నుండి మీ ధరించగలిగే గాడ్జెట్‌లోని సున్నితమైన డేటాను మీరు ఎలా రక్షించగలరు?

ఎ) ధరించగలిగే గాడ్జెట్‌ల వాడకాన్ని పూర్తిగా నివారించడం ద్వారా

బి) పరికర యాక్సెస్ కోసం బలమైన పాస్‌కోడ్‌లు లేదా పిన్‌లను ప్రారంభించడం ద్వారా

సి) బాహ్య కార్యకలాపాల కోసం ధరించగలిగే గాడ్జెట్‌లను మాత్రమే ఉపయోగించడం ద్వారా

D) మద్దతు కోసం స్నేహితులు మరియు కుటుంబ సభ్యులతో వ్యక్తిగత ఆరోగ్య డేటాను పంచుకోవడం ద్వారా

సమాధానం: బి) పరికర యాక్సెస్ కోసం బలమైన పాస్‌కోడ్‌లు లేదా పిన్‌లను ప్రారంభించడం ద్వారా

ప్రశ్న 8:

ధరించగలిగే గాడ్జెట్‌ల భద్రత విషయంలో "ధరించదగిన పరికరం జత చేయడం" అంటే ఏమిటి?

ఎ) కార్యాచరణను మెరుగుపరచడానికి ధరించగలిగే రెండు గాడ్జెట్‌లను జత చేసే పద్ధతి

B) కమ్యూనికేషన్ మరియు డేటా సింక్రొనైజేషన్ కోసం ధరించగలిగే పరికరాన్ని స్మార్ట్‌ఫోన్ లేదా మరొక పరికరంతో జత చేసే ప్రక్రియ

సి) నష్టం జరిగినప్పుడు ధరించగలిగే గాడ్జెట్ స్థానాన్ని ట్రాక్ చేయడానికి ఉపయోగించే సాంకేతికత

D) ధరించగలిగిన గాడ్జెట్‌ని కంప్యూటర్‌కు కనెక్ట్ చేయడం ద్వారా దాని పనితీరును మెరుగుపరచడానికి ఒక మార్గం

సమాధానం: బి) కమ్యూనికేషన్ మరియు డేటా సమకాలీకరణ కోసం ధరించగలిగే పరికరాన్ని స్మార్ట్‌ఫోన్ లేదా మరొక పరికరంతో జత చేసే ప్రక్రియ

ప్రశ్న 9:

మీ ధరించగలిగిన గాడ్జెట్‌ను హ్యాక్ చేయకుండా లేదా రాజీ పడకుండా మీరు ఎలా రక్షించుకోవచ్చు?

ఎ) గాడ్జెట్‌ను ప్రతిరోజూ పరిమిత వ్యవధిలో మాత్రమే ఉపయోగించడం ద్వారా

బి) అదనపు రక్షణ కోసం గాడ్జెట్‌లో బహుళ యాంటీవైరస్ యాప్‌లను ఇన్‌స్టాల్ చేయడం ద్వారా

సి) అసురక్షిత పబ్లిక్ Wi-Fi నెట్‌వర్క్‌లకు గాడ్జెట్‌ను కనెక్ట్ చేయడంలో జాగ్రత్తగా ఉండటం ద్వారా

D) మీ ధరించగలిగే గాడ్జెట్‌ని స్నేహితులు మరియు కుటుంబ సభ్యులతో సరదాగా పంచుకోవడం ద్వారా

సమాధానం: సి) గాడ్జెట్‌ను అసురక్షిత పబ్లిక్ Wi-Fi నెట్‌వర్క్‌లకు కనెక్ట్ చేయడంలో జాగ్రత్తగా ఉండటం ద్వారా

ప్రశ్న 10:

మీరు మీ ధరించగలిగే గాడ్జెట్‌లో అసాధారణమైన లేదా అనుమానాస్పద ప్రవర్తనను ఎదుర్కొంటే మీరు ఏమి చేయాలి?

ఎ) స్నేహితుల నుండి సలహా కోసం సోషల్ మీడియాలో సంఘటనను పంచుకోండి

బి) గాడ్జెట్‌ని ఉపయోగించడం కొనసాగించండి మరియు ప్రవర్తన దానంతటదే ఆగిపోతుందని ఆశిస్తున్నాము

సి) సమస్యను పరిష్కరించడానికి గాడ్జెట్‌లో ఫ్యాక్టరీ రీసెట్ చేయండి

D) సహాయం కోసం గాడ్జెట్ తయారీదారుని లేదా కస్టమర్ మద్దతును సంప్రదించండి

సమాధానం: D) సహాయం కోసం గాడ్జెట్ తయారీదారుని లేదా కస్టమర్ మద్దతును సంప్రదించండి

Day – 5

**ఆరోగ్య సమస్యలు (కళ్ళు)**

ప్రశ్న 1:

డిజిటల్ పరికరాలను ఎక్కువసేపు ఉపయోగించడం వల్ల కళ్లకు సంబంధించిన కొన్ని ఆరోగ్య సమస్యలు ఏమిటి?

ఎ) బరువు పెరగడం మరియు ఊబకాయం

బి) కార్పల్ టన్నెల్ సిండ్రోమ్

సి) కంప్యూటర్ విజన్ సిండ్రోమ్ (CVS) లేదా డిజిటల్ ఐ స్ట్రెయిన్

డి) వినికిడి లోపం

జవాబు: సి) కంప్యూటర్ విజన్ సిండ్రోమ్ (CVS) లేదా డిజిటల్ ఐ స్ట్రెయిన్

ప్రశ్న 2:

కంప్యూటర్ విజన్ సిండ్రోమ్ (CVS) యొక్క సాధారణ లక్షణాలు ఏమిటి?

ఎ) కండరాల నొప్పి మరియు వెన్నునొప్పి

బి) కళ్లు పొడిబారడం, కంటి ఒత్తిడి, తలనొప్పి

సి) మైకము మరియు వికారం

D) వేళ్లలో జలదరింపు లేదా తిమ్మిరి

జవాబు: బి) కళ్లు పొడిబారడం, కంటి ఒత్తిడి, తలనొప్పి

ప్రశ్న 3:

ఎక్కువసేపు స్క్రీన్ సమయం డిజిటల్ కంటి ఒత్తిడిని ఎందుకు కలిగిస్తుంది?

ఎ) డిజిటల్ స్క్రీన్‌లు హానికరమైన అతినీలలోహిత (UV) కిరణాలను విడుదల చేస్తాయి

బి) స్క్రీన్‌ల వైపు చూడటం వలన కంటికి సరిగ్గా దృష్టి కేంద్రీకరించే సామర్థ్యం తగ్గుతుంది

సి) డిజిటల్ స్క్రీన్‌లు కళ్లకు చికాకు కలిగించే విషపూరిత పొగలను విడుదల చేస్తాయి

డి) స్క్రీన్‌లను ఉపయోగించడం వల్ల కళ్లకు రక్త ప్రసరణ తగ్గుతుంది

జవాబు: బి) స్క్రీన్‌ల వైపు చూస్తూ ఉండడం వల్ల కంటికి సరిగ్గా దృష్టి సారించగల సామర్థ్యం తగ్గుతుంది

ప్రశ్న 4:

20-20-20 నియమం అంటే ఏమిటి మరియు ఇది డిజిటల్ కంటి ఒత్తిడిని నివారించడంలో ఎలా సహాయపడుతుంది?

ఎ) 20-20-20 నియమం ప్రతి 20 నిమిషాలకు డిజిటల్ పరికరాల నుండి విరామం తీసుకోవాలని మరియు కంటి ఒత్తిడిని తగ్గించడానికి 20 సెకన్ల పాటు 20 అడుగుల దూరంలో ఉన్నదాన్ని చూడాలని సూచిస్తుంది.

B) 20-20-20 నియమం డిజిటల్ పరికరాలను నిరంతరం 20 నిమిషాల పాటు ఉపయోగించడాన్ని ప్రోత్సహిస్తుంది, తర్వాత 20-సెకన్ల విరామం, 20 సార్లు పునరావృతమవుతుంది.

సి) 20-20-20 నియమం కళ్ళను రక్షించడానికి ప్రతి 20 నిమిషాలకు స్క్రీన్ ప్రకాశాన్ని 20%కి తగ్గించాలని సలహా ఇస్తుంది.

డి) 20-20-20 నియమం వాటిని విశ్రాంతి తీసుకోవడానికి ప్రతి 20 నిమిషాలకు 20 సెకన్ల పాటు కళ్ళు మూసుకుని ఉండాలని సలహా ఇస్తుంది.

సమాధానం: ఎ) 20-20-20 నియమం ప్రతి 20 నిమిషాలకు డిజిటల్ పరికరాల నుండి విరామం తీసుకోవాలని మరియు కంటి ఒత్తిడిని తగ్గించడానికి 20 సెకన్ల పాటు 20 అడుగుల దూరంలో ఉన్నదాన్ని చూడాలని సూచిస్తుంది.

ప్రశ్న 5:

"బ్లూ లైట్" అంటే ఏమిటి మరియు ఇది కళ్ళను ఎలా ప్రభావితం చేస్తుంది?

ఎ) బ్లూ లైట్ అనేది దృష్టిని మెరుగుపరచడానికి నేత్ర వైద్య చికిత్సలలో ఉపయోగించే ఒక రకమైన కాంతి.

బి) బ్లూ లైట్ అనేది సహజ కాంతి స్పెక్ట్రం, ఇది కళ్ళకు ప్రయోజనం చేకూరుస్తుంది మరియు దృష్టిని మెరుగుపరుస్తుంది.

సి) బ్లూ లైట్ అనేది డిజిటల్ స్క్రీన్‌ల ద్వారా విడుదలయ్యే అధిక-శక్తి కనిపించే కాంతి, ఇది కంటి ఒత్తిడిని కలిగిస్తుంది మరియు నిద్ర విధానాలకు అంతరాయం కలిగిస్తుంది.

డి) బ్లూ లైట్ అనేది కంటి పరిస్థితులకు చికిత్స చేయడానికి ఉపయోగించే ఒక రకమైన కాంతి చికిత్స.

సమాధానం: సి) బ్లూ లైట్ అనేది డిజిటల్ స్క్రీన్‌ల ద్వారా విడుదలయ్యే అధిక-శక్తి కనిపించే కాంతి, ఇది కంటి ఒత్తిడిని కలిగిస్తుంది మరియు నిద్ర విధానాలకు అంతరాయం కలిగిస్తుంది.

ప్రశ్న 6:

"డిజిటల్ కంటి అలసట" అంటే ఏమిటి మరియు దానిని ఎలా తగ్గించవచ్చు?

ఎ) డిజిటల్ ఐ ఫెటీగ్ అనేది అధిక స్క్రీన్ సమయం నుండి కళ్ళు శారీరకంగా అలసిపోయే పరిస్థితి. స్క్రీన్ బ్రైట్‌నెస్‌ని తగ్గించడం ద్వారా దీనిని తగ్గించవచ్చు.

బి) డిజిటల్ ఐ ఫెటీగ్ అనేది ఎక్కువ కాలం పాటు డిజిటల్ పరికరాలను ఉపయోగించిన తర్వాత కళ్లు బరువుగా మరియు అలసటగా అనిపించే పరిస్థితి. కంటి చుక్కలను క్రమం తప్పకుండా ఉపయోగించడం ద్వారా దీనిని తగ్గించవచ్చు.

సి) డిజిటల్ ఐ ఫెటీగ్ అనేది అధిక స్క్రీన్ సమయం నుండి కళ్ళు పొడిగా మరియు చికాకుగా మారే పరిస్థితి. 20-20-20 నియమాన్ని అనుసరించడం మరియు తరచుగా విరామాలు తీసుకోవడం ద్వారా దీనిని తగ్గించవచ్చు.

డి) డిజిటల్ ఐ ఫెటీగ్ అనేది అధిక స్క్రీన్ సమయం నుండి కళ్ళు ఎర్రగా మరియు రక్తం కారుతున్న స్థితి. కళ్లపై వెచ్చని కంప్రెస్‌లను ఉపయోగించడం ద్వారా దీనిని తగ్గించవచ్చు.

జవాబు: సి) డిజిటల్ ఐ ఫెటీగ్ అనేది అధిక స్క్రీన్ సమయం నుండి కళ్ళు పొడిగా మరియు చికాకుగా మారే పరిస్థితి. 20-20-20 నియమాన్ని అనుసరించడం మరియు తరచుగా విరామాలు తీసుకోవడం ద్వారా దీనిని తగ్గించవచ్చు.

ప్రశ్న 7:

డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు సరైన లైటింగ్ యొక్క ప్రాముఖ్యత ఏమిటి?

ఎ) ప్రకాశవంతమైన లైటింగ్ స్క్రీన్ దృశ్యమానతను మెరుగుపరుస్తుంది మరియు కంటి ఒత్తిడిని తగ్గిస్తుంది.

బి) డిమ్ లైటింగ్ ఎక్కువసేపు స్క్రీన్ సమయంలో కళ్లకు విశ్రాంతినిస్తుంది.

సి) సరైన లైటింగ్ స్క్రీన్‌పై కాంతి మరియు ప్రతిబింబాలను తగ్గిస్తుంది, కంటి ఒత్తిడిని తగ్గిస్తుంది.

డి) డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు ఉపయోగించిన లైటింగ్ రకం కంటి ఆరోగ్యాన్ని ప్రభావితం చేయదు.

సమాధానం: సి) సరైన లైటింగ్ స్క్రీన్‌పై కాంతిని మరియు ప్రతిబింబాలను తగ్గిస్తుంది, కంటి ఒత్తిడిని తగ్గిస్తుంది.

ప్రశ్న 8:

మీ కళ్ళపై నీలి కాంతి ప్రభావాన్ని తగ్గించడానికి మీరు ఏమి చేయవచ్చు?

ఎ) మీ డిజిటల్ పరికరంలో బ్లూ లైట్ ఫిల్టర్‌ను ఇన్‌స్టాల్ చేయండి.

B) బ్లూ లైట్ ప్రభావాలను ఎదుర్కోవడానికి స్క్రీన్ ప్రకాశాన్ని పెంచండి.

సి) బ్లూ లైట్ ఎక్స్‌పోజర్‌ను నివారించడానికి పూర్తి చీకటిలో డిజిటల్ పరికరాలను ఉపయోగించండి.

డి) బ్లూ లైట్ ఎక్స్‌పోజర్‌ని మెరుగుపరచడానికి నీలిరంగు అద్దాలను ఉపయోగించండి.

సమాధానం: ఎ) మీ డిజిటల్ పరికరంలో బ్లూ లైట్ ఫిల్టర్‌ని ఇన్‌స్టాల్ చేయండి.

ప్రశ్న 9:

డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు స్క్రీన్ నుండి తగిన దూరాన్ని నిర్వహించడం ఎందుకు ముఖ్యం?

ఎ) తగిన దూరాన్ని నిర్వహించడం పరికరంలో బ్యాటరీ వినియోగాన్ని తగ్గించడంలో సహాయపడుతుంది.

బి) డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు స్క్రీన్ నుండి దూరం కంటి ఆరోగ్యంపై ప్రభావం చూపదు.

సి) తగిన దూరాన్ని నిర్వహించడం కంటి ఒత్తిడి మరియు అలసటను తగ్గిస్తుంది.

D) స్క్రీన్‌కి చాలా దగ్గరగా కూర్చోవడం వల్ల దృశ్యమానత మరియు దృష్టిని మెరుగుపరచడంలో సహాయపడుతుంది.

జవాబు: సి) తగిన దూరం పాటించడం వల్ల కంటి ఒత్తిడి మరియు అలసట తగ్గుతుంది.

ప్రశ్న 10:

డిజిటల్ పరికర వినియోగానికి సంబంధించి కంటి ఆరోగ్యానికి సాధారణ కంటి పరీక్షలు ఎలా సహాయపడతాయి?

ఎ) రెగ్యులర్ కంటి పరీక్షలు డిజిటల్ పరికరాలను ఉపయోగించాల్సిన అవసరాన్ని నిరోధించవచ్చు.

బి) రెగ్యులర్ కంటి పరీక్షలు డిజిటల్ పరికర వినియోగం వల్ల కలిగే దృష్టి సమస్యలను గుర్తించి పరిష్కరించగలవు.

సి) రెగ్యులర్ కంటి పరీక్షలు డిజిటల్ స్క్రీన్‌ల రంగు ఖచ్చితత్వం మరియు పదును మెరుగుపరుస్తాయి.

డి) రెగ్యులర్ కంటి పరీక్షలు డిజిటల్ పరికరాల ద్వారా వెలువడే నీలి కాంతిని తగ్గించగలవు.

జవాబు: బి) రెగ్యులర్ కంటి పరీక్షలు డిజిటల్ పరికర వినియోగం వల్ల కలిగే దృష్టి సమస్యలను గుర్తించి పరిష్కరించగలవు.

**మానసిక ఆరోగ్య**

ప్రశ్న 1:

డిజిటల్ పరికరాల అధిక వినియోగంతో సంబంధం ఉన్న కొన్ని మానసిక ఆరోగ్య సమస్యలు ఏమిటి?

ఎ) పెరిగిన సామాజిక పరస్పర చర్యలు మరియు మెరుగైన మానసిక శ్రేయస్సు

బి) ఒత్తిడి మరియు ఆందోళన స్థాయిలను తగ్గించడం

సి) డిజిటల్ వ్యసనం, సామాజిక ఒంటరితనం మరియు ఆందోళన

D) మెరుగైన ఉత్పాదకత మరియు ఏకాగ్రత

సమాధానం: సి) డిజిటల్ వ్యసనం, సామాజిక ఒంటరితనం మరియు ఆందోళన

ప్రశ్న 2:

మానసిక ఆరోగ్యం కోసం స్క్రీన్ సమయం మరియు డిజిటల్ పరికర వినియోగాన్ని గుర్తుంచుకోవడం ఎందుకు ముఖ్యం?

ఎ) డిజిటల్ పరికరాలు మానసిక ఆరోగ్య సమస్యలను నయం చేయగలవు మరియు చికిత్సా ప్రయోజనాలను అందిస్తాయి

బి) మెరుగైన మానసిక శ్రేయస్సు కోసం రెగ్యులర్ డిజిటల్ పరికర వినియోగం అవసరం

సి) అధిక స్క్రీన్ సమయం ఒత్తిడిని పెంచుతుంది మరియు నిద్ర విధానాలకు అంతరాయం కలిగిస్తుంది

డి) స్క్రీన్ సమయం మరియు డిజిటల్ పరికర వినియోగం ద్వారా మానసిక ఆరోగ్యం ప్రభావితం కాదు

సమాధానం: సి) అధిక స్క్రీన్ సమయం ఒత్తిడిని పెంచడానికి మరియు నిద్ర విధానాలకు అంతరాయం కలిగించడానికి దారితీస్తుంది

ప్రశ్న 3:

"డిజిటల్ డిటాక్స్" అంటే ఏమిటి మరియు అది మానసిక ఆరోగ్యానికి ఎలా ఉపయోగపడుతుంది?

ఎ) డిజిటల్ డిటాక్స్ మానసిక ఆరోగ్యాన్ని మెరుగుపరచడానికి డిజిటల్ పరికరాలను ఎక్కువ కాలం ఉపయోగించడాన్ని సూచిస్తుంది

బి) డిజిటల్ డిటాక్స్ అనేది ఒత్తిడిని తగ్గించడానికి మరియు సంపూర్ణతను ప్రోత్సహించడానికి డిజిటల్ పరికర వినియోగాన్ని పరిమితం చేసే ప్రక్రియ

సి) డిజిటల్ డిటాక్స్ అనేది శారీరక ఆరోగ్యాన్ని మెరుగుపరచడానికి సోషల్ మీడియా నుండి డిస్‌కనెక్ట్ చేయడం

డి) డిజిటల్ డిటాక్స్ మానసిక ఆరోగ్యం మరియు శ్రేయస్సుపై ఎటువంటి ప్రభావం చూపదు

జవాబు: బి) డిజిటల్ డిటాక్స్ అనేది ఒత్తిడిని తగ్గించడానికి మరియు సంపూర్ణతను ప్రోత్సహించడానికి డిజిటల్ పరికర వినియోగాన్ని పరిమితం చేసే ప్రక్రియ

ప్రశ్న 4:

సోషల్ మీడియా ఉపయోగం మరియు మానసిక ఆరోగ్యం మధ్య సంభావ్య సంబంధం ఏమిటి?

ఎ) పెరిగిన సోషల్ మీడియా వినియోగం నేరుగా మెరుగైన మానసిక శ్రేయస్సుతో ముడిపడి ఉంటుంది

బి) సోషల్ మీడియా వాడకం మానసిక ఆరోగ్యంపై ఎలాంటి ప్రభావం చూపదు

సి) అధిక సోషల్ మీడియా వాడకం ఒంటరితనం, నిరాశ మరియు ఆందోళన వంటి భావాలకు దోహదం చేస్తుంది

డి) సోషల్ మీడియా వినియోగం నిజ జీవిత సామాజిక పరస్పర చర్యలను భర్తీ చేస్తుంది మరియు మానసిక ఆరోగ్యాన్ని మెరుగుపరుస్తుంది

సమాధానం: సి) అధిక సోషల్ మీడియా వినియోగం ఒంటరితనం, నిరాశ మరియు ఆందోళన వంటి భావాలకు దోహదం చేస్తుంది

ప్రశ్న 5:

డిజిటల్ పరికరాల నిరంతర ఉపయోగం నిద్ర మరియు మానసిక ఆరోగ్యాన్ని ఎలా ప్రభావితం చేస్తుంది?

ఎ) డిజిటల్ పరికరాలను క్రమం తప్పకుండా ఉపయోగించడం వల్ల నిద్ర నాణ్యత మరియు మొత్తం మానసిక ఆరోగ్యం మెరుగుపడుతుంది

బి) డిజిటల్ పరికరాలు నిద్ర విధానాలు లేదా మానసిక ఆరోగ్యంపై ప్రభావం చూపవు

సి) ముఖ్యంగా నిద్రవేళకు ముందు స్క్రీన్‌లకు నిరంతరం బహిర్గతం కావడం నిద్రకు భంగం కలిగించవచ్చు మరియు మానసిక ఆరోగ్యాన్ని ప్రతికూలంగా ప్రభావితం చేస్తుంది

డి) డిజిటల్ పరికరాలు నిద్ర విధానాలను నియంత్రించడంలో మరియు మానసిక ఆరోగ్య సమస్యల ప్రమాదాన్ని తగ్గించడంలో సహాయపడతాయి.

ప్రశ్న 6:

"నోమోఫోబియా" అంటే ఏమిటి మరియు అది మానసిక ఆరోగ్యాన్ని ఎలా ప్రభావితం చేస్తుంది?

ఎ) ఒకరి మొబైల్ పరికరం లేకుండా ఉండాలనే భయం, ఇది పెరిగిన ఒత్తిడి మరియు ఆందోళనకు దారితీస్తుంది

బి) వ్యక్తిగతంగా సాంఘికీకరించే భయం, తగ్గిన సామాజిక ఒత్తిళ్ల కారణంగా మానసిక ఆరోగ్యం మెరుగుపడుతుంది

సి) డిజిటల్ పరికరాల భయం, ఇది స్క్రీన్ సమయాన్ని తగ్గించడం ద్వారా మానసిక ఆరోగ్యాన్ని మెరుగుపరుస్తుంది

D) ధ్వనించే వాతావరణంలో ఉండటం వలన కలిగే భయం, ఇది మెరుగైన మానసిక శ్రేయస్సుకు దారితీస్తుంది

జవాబు: ఎ) ఒకరి మొబైల్ పరికరం లేకుండా ఉండాలనే భయం, ఇది పెరిగిన ఒత్తిడి మరియు ఆందోళనకు దారితీస్తుంది

ప్రశ్న 7:

మెరుగైన మానసిక ఆరోగ్యం కోసం సరిహద్దులను సెట్ చేయడం మరియు డిజిటల్ పరికర వినియోగాన్ని నిర్వహించడం ఎందుకు అవసరం?

ఎ) సరిహద్దులను నిర్ణయించడం వల్ల శారీరక ఆరోగ్యాన్ని మెరుగుపరుస్తుంది కానీ మానసిక ఆరోగ్యంపై ఎలాంటి ప్రభావం ఉండదు

బి) డిజిటల్ పరికర వినియోగాన్ని నిర్వహించడం మానసిక ఆరోగ్యం మరియు శ్రేయస్సుపై ఎటువంటి ప్రభావం చూపదు

సి) సరిహద్దులను ఏర్పరుచుకోవడం వలన డిజిటల్ పరికరాలకు సంబంధించిన ఒత్తిడి, ఆందోళన మరియు భారాన్ని తగ్గించవచ్చు

డి) డిజిటల్ పరికర వినియోగానికి సరిహద్దులను సెట్ చేయడం వ్యసనానికి మరియు సాంకేతికతపై ఆధారపడటానికి దారితీస్తుంది

జవాబు: సి) సరిహద్దులను ఏర్పరచుకోవడం వలన డిజిటల్ పరికరాలకు సంబంధించిన ఒత్తిడి, ఆందోళన మరియు అధికమైన భావాలను తగ్గించవచ్చు

ప్రశ్న 8:

డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు మానసిక ఆరోగ్యాన్ని పెంపొందించడంలో బుద్ధిపూర్వక అభ్యాసాలు ఎలా సహాయపడతాయి?

ఎ) డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు మానసిక ఆరోగ్యానికి మైండ్‌ఫుల్‌నెస్ పద్ధతులు ప్రభావవంతంగా ఉండవు

బి) డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు మైండ్‌ఫుల్‌నెస్ దృష్టి మరియు ఉత్పాదకతను మెరుగుపరుస్తుంది

సి) డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు బుద్ధిపూర్వకంగా పాల్గొనడం ఒత్తిడిని తగ్గిస్తుంది మరియు మొత్తం మానసిక శ్రేయస్సును మెరుగుపరుస్తుంది

D) మైండ్‌ఫుల్‌నెస్ అభ్యాసాలు స్క్రీన్ సమయాన్ని పెంచడానికి మరియు మానసిక ఆరోగ్యాన్ని మెరుగుపరచడంలో సహాయపడతాయి

ప్రశ్న 9:

డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు మీ మానసిక ఆరోగ్యానికి మద్దతు ఇవ్వడానికి మీరు ఏమి చేయవచ్చు?

ఎ) మానసిక ఆరోగ్య సమస్యలను నివారించడానికి డిజిటల్ పరికరాలను పూర్తిగా ఉపయోగించడం మానుకోండి

B) శ్రేయస్సును ప్రోత్సహించడానికి డిజిటల్ పరికరాల నుండి తరచుగా విరామం తీసుకోండి మరియు ఇతర కార్యకలాపాలలో పాల్గొనండి

సి) ఇతరులతో కనెక్ట్ అవ్వడానికి మరియు ఒంటరితనం యొక్క భావాలను తగ్గించడానికి సోషల్ మీడియాలో ఎక్కువ సమయం గడపండి

డి) కనెక్ట్ అయి ఉండటానికి మరియు ఆందోళనను తగ్గించడానికి డిజిటల్ పరికరాలను ఎల్లప్పుడూ సమీపంలో ఉంచండి

జవాబు: బి) శ్రేయస్సును ప్రోత్సహించడానికి డిజిటల్ పరికరాల నుండి తరచుగా విరామం తీసుకోండి మరియు ఇతర కార్యకలాపాలలో పాల్గొనండి

ప్రశ్న 10:

ఆన్‌లైన్ మరియు ఆఫ్‌లైన్ కార్యకలాపాల మధ్య ఆరోగ్యకరమైన సమతుల్యతను కాపాడుకోవడం మానసిక ఆరోగ్యానికి ఎలా ఉపయోగపడుతుంది?

ఎ) సమతుల్య విధానం డిజిటల్ వ్యసనం మరియు డిపెండెన్సీని మెరుగుపరచడంలో సహాయపడుతుంది

బి) ఆన్‌లైన్ మరియు ఆఫ్‌లైన్ కార్యకలాపాల మధ్య సమతుల్యతను సాధించడం సామాజిక ఒంటరితనం యొక్క భావాలను తగ్గిస్తుంది మరియు మానసిక ఆరోగ్యాన్ని మెరుగుపరుస్తుంది

సి) ఆన్‌లైన్ కార్యకలాపాలపై మాత్రమే దృష్టి కేంద్రీకరించడం వల్ల మానసిక ఉల్లాసం మెరుగుపడుతుంది

డి) ఆన్‌లైన్‌లో ఎక్కువ సమయం గడపడం వల్ల ఒత్తిడి మరియు ఆందోళన స్థాయిలు తగ్గుతాయి

సమాధానం: బి) ఆన్‌లైన్ మరియు ఆఫ్‌లైన్ కార్యకలాపాల మధ్య సమతుల్యతను సాధించడం సామాజిక ఒంటరి భావాలను తగ్గిస్తుంది మరియు మానసిక ఆరోగ్యాన్ని మెరుగుపరుస్తుంది

**శారీరక ఆరోగ్యం**

ప్రశ్న 1:

డిజిటల్ పరికరాల అధిక వినియోగంతో సంబంధం ఉన్న కొన్ని శారీరక ఆరోగ్య సమస్యలు ఏమిటి?

ఎ) పెరిగిన శారీరక దృఢత్వం మరియు కండరాల బలం

బి) మెరుగైన భంగిమ మరియు మస్క్యులోస్కెలెటల్ సమస్యల ప్రమాదాన్ని తగ్గిస్తుంది

సి) డిజిటల్ కంటి ఒత్తిడి, మెడ మరియు భుజం నొప్పి, మరియు టెక్స్ట్ మెడ

D) మెరుగైన హృదయనాళ ఆరోగ్యం మరియు ఊబకాయం తగ్గిన ప్రమాదం

సమాధానం: సి) డిజిటల్ కంటి ఒత్తిడి, మెడ మరియు భుజం నొప్పి మరియు టెక్స్ట్ మెడ

ప్రశ్న 2:

"టెక్స్ట్ నెక్" అంటే ఏమిటి మరియు ఇది డిజిటల్ పరికరాలకు ఎలా సంబంధం కలిగి ఉంటుంది?

ఎ) టెక్స్ట్ నెక్ అనేది నడుస్తున్నప్పుడు టెక్స్ట్ చేసే చర్యను సూచిస్తుంది, ఇది ప్రమాదాలు మరియు గాయాలకు దారితీయవచ్చు.

బి) టెక్స్ట్ నెక్ అనేది మెడ మరియు పైభాగంలో నొప్పి మరియు ఒత్తిడిని తలక్రిందులుగా ఉంచి డిజిటల్ పరికరాలను దీర్ఘకాలం ఉపయోగించడం వల్ల కలుగుతుంది.

సి) టెక్స్ట్ నెక్ అనేది తరచుగా టెక్స్ట్ చేయడం వల్ల మెడ కండరాలు బలంగా మరియు మరింత అభివృద్ధి చెందే పరిస్థితి.

డి) టెక్స్ట్ నెక్ అనేది టెక్స్టింగ్‌కు సంబంధించిన ఒక పరిస్థితి, ఇది శారీరక ఆరోగ్యంపై ఎలాంటి ప్రభావం చూపదు.

జవాబు: బి) టెక్స్ట్ నెక్ అనేది మెడ మరియు పైభాగంలో నొప్పి మరియు ఒత్తిడిని తలక్రిందులుగా ఉంచి డిజిటల్ పరికరాలను దీర్ఘకాలం ఉపయోగించడం వల్ల ఏర్పడుతుంది.

ప్రశ్న 3:

డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు సరైన ఎర్గోనామిక్ సెటప్‌ను నిర్వహించడం ఎందుకు ముఖ్యం?

ఎ) డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు సరైన ఎర్గోనామిక్ సెటప్ శారీరక ఆరోగ్యంపై ప్రభావం చూపదు.

బి) ఎర్గోనామిక్ సెటప్ డిజిటల్ పరికర పనితీరు మరియు బ్యాటరీ జీవితాన్ని మెరుగుపరుస్తుంది.

సి) ఎర్గోనామిక్ సెటప్ మస్క్యులోస్కెలెటల్ సమస్యలు మరియు శారీరక అసౌకర్యాల ప్రమాదాన్ని తగ్గించడంలో సహాయపడుతుంది.

డి) ఎర్గోనామిక్ సెటప్‌లో డిజిటల్ పరికరాలను ఉపయోగించడం డిజిటల్ వ్యసనం మరియు డిపెండెన్సీకి దారి తీస్తుంది.

సమాధానం: సి) ఎర్గోనామిక్ సెటప్ మస్క్యులోస్కెలెటల్ సమస్యలు మరియు శారీరక అసౌకర్యాల ప్రమాదాన్ని తగ్గించడంలో సహాయపడుతుంది.

జవాబు: B) RSI అనేది టైపింగ్ మరియు స్వైపింగ్ వంటి డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు పునరావృతమయ్యే కదలికల ఫలితంగా ఏర్పడే పరిస్థితి.

ప్రశ్న 5:

డిజిటల్ పరికరాలను దీర్ఘకాలం ఉపయోగించడం వల్ల చేతి మరియు మణికట్టు ఆరోగ్యాన్ని ఎలా ప్రభావితం చేయవచ్చు?

ఎ) విస్తరించిన డిజిటల్ పరికర వినియోగం చేతి మరియు మణికట్టు కండరాలను బలోపేతం చేస్తుంది.

బి) డిజిటల్ పరికరాలు చేతి మరియు మణికట్టు ఆరోగ్యంపై ప్రభావం చూపవు.

సి) డిజిటల్ పరికరాలను దీర్ఘకాలం ఉపయోగించడం వల్ల చేతి మరియు మణికట్టు నొప్పి, దృఢత్వం మరియు కార్పల్ టన్నెల్ సిండ్రోమ్ వంటి సంభావ్య గాయాలకు దారితీయవచ్చు.

డి) డిజిటల్ పరికరాలను ఉపయోగించడం వలన చేతి మరియు మణికట్టు సమస్యల ప్రమాదాన్ని తగ్గించడం ద్వారా చేతి-కంటి సమన్వయాన్ని మెరుగుపరుస్తుంది.

సమాధానం: సి) డిజిటల్ పరికరాలను దీర్ఘకాలం ఉపయోగించడం వల్ల చేతి మరియు మణికట్టు నొప్పి, దృఢత్వం మరియు కార్పల్ టన్నెల్ సిండ్రోమ్ వంటి సంభావ్య గాయాలకు దారితీయవచ్చు.

ప్రశ్న 6:

డిజిటల్ పరికర వినియోగానికి సంబంధించిన శారీరక ఆరోగ్య సమస్యలను నివారించడానికి కొన్ని సంభావ్య మార్గాలు ఏమిటి?

ఎ) శారీరక ఆరోగ్య సమస్యలను నివారించడానికి డిజిటల్ పరికరాలను పూర్తిగా ఉపయోగించకుండా ఉండండి.

బి) డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు తరచుగా విరామం తీసుకోండి, సరైన భంగిమను నిర్వహించండి మరియు సాగదీయడం వ్యాయామాలు చేయండి.

సి) కండరాలను బలోపేతం చేయడానికి మరియు శారీరక ఆరోగ్యాన్ని మెరుగుపరచడానికి ఎక్కువ కాలం డిజిటల్ పరికరాలను ఉపయోగించండి.

డి) డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు ఎలాంటి శారీరక అసౌకర్యాన్ని అనుభవించినా పట్టించుకోకండి.

సమాధానం: బి) డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు తరచుగా విరామం తీసుకోండి, సరైన భంగిమను నిర్వహించండి మరియు సాగదీయడం వ్యాయామాలు చేయండి.

ప్రశ్న 8:

డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు సుదీర్ఘమైన నిశ్చల ప్రవర్తనను నివారించడం ఎందుకు ముఖ్యం?

ఎ) డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు నిశ్చల ప్రవర్తన శారీరక ఆరోగ్యంపై ప్రభావం చూపదు.

బి) సుదీర్ఘమైన నిశ్చల ప్రవర్తన స్థూలకాయం, హృదయ సంబంధ సమస్యలు మరియు చలనశీలత తగ్గడం వంటి శారీరక ఆరోగ్య సమస్యలకు దారితీస్తుంది.

సి) నిశ్చల స్థితిలో డిజిటల్ పరికరాలను ఉపయోగించడం డిజిటల్ వ్యసనం మరియు ఆధారపడటాన్ని పెంచుతుంది.

D) సుదీర్ఘమైన నిశ్చల ప్రవర్తన కండరాలను బలోపేతం చేస్తుంది మరియు శారీరక ఆరోగ్యాన్ని మెరుగుపరుస్తుంది.

సమాధానం: బి) సుదీర్ఘమైన నిశ్చల ప్రవర్తన వల్ల స్థూలకాయం, హృదయ సంబంధ సమస్యలు మరియు చలనశీలత తగ్గడం వంటి శారీరక ఆరోగ్య సమస్యలకు దారితీయవచ్చు.

ప్రశ్న 9:

డిజిటల్ పరికరాల నుండి వచ్చే నీలి కాంతి శారీరక ఆరోగ్యాన్ని, ముఖ్యంగా నిద్రను ఎలా ప్రభావితం చేస్తుంది?

ఎ) డిజిటల్ పరికరాల నుండి బ్లూ లైట్ ఎక్స్పోజర్ నిద్ర నాణ్యతను మెరుగుపరుస్తుంది మరియు నిద్ర ఆటంకాలను తగ్గిస్తుంది.

B) బ్లూ లైట్ శారీరక ఆరోగ్యం లేదా నిద్ర విధానాలపై ప్రభావం చూపదు.

సి) డిజిటల్ పరికరాల నుండి బ్లూ లైట్ ఎక్స్పోజర్ నిద్ర విధానాలకు భంగం కలిగిస్తుంది మరియు శారీరక ఆరోగ్యాన్ని ప్రతికూలంగా ప్రభావితం చేస్తుంది.

డి) బ్లూ లైట్ ఫిల్టర్‌లతో డిజిటల్ పరికరాలను ఉపయోగించడం వల్ల శారీరక ఆరోగ్యం మెరుగుపడుతుంది.

సమాధానం: సి) డిజిటల్ పరికరాల నుండి బ్లూ లైట్ బహిర్గతం నిద్ర విధానాలకు భంగం కలిగిస్తుంది మరియు శారీరక ఆరోగ్యాన్ని ప్రతికూలంగా ప్రభావితం చేస్తుంది.

ప్రశ్న 10:

డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు మెరుగైన శారీరక ఆరోగ్యాన్ని ప్రోత్సహించడానికి మీరు ఏమి చేయవచ్చు?

ఎ) శారీరక శ్రమను తగ్గించడానికి తక్కువ లైటింగ్‌తో చీకటి గదుల్లో డిజిటల్ పరికరాలను ఉపయోగించండి.

బి) డిజిటల్ పరికరాల నుండి క్రమం తప్పకుండా విరామం తీసుకోండి, సరైన భంగిమను ప్రాక్టీస్ చేయండి మరియు శారీరక శ్రమలో పాల్గొనండి.

సి) భౌతిక ఆరోగ్యం మరియు శ్రేయస్సును మెరుగుపరచడానికి డిజిటల్ పరికరాలను ఉపయోగించి ఎక్కువ సమయాన్ని వెచ్చించండి.

డి) డిజిటల్ పరికరాలను ఉపయోగిస్తున్నప్పుడు ఎలాంటి శారీరక అసౌకర్యాన్ని అనుభవించినా పట్టించుకోకండి.

సమాధానం: బి) డిజిటల్ పరికరాల నుండి క్రమం తప్పకుండా విరామం తీసుకోండి, సరైన భంగిమను అభ్యసించండి మరియు శారీరక శ్రమలో పాల్గొనండి.

**కంప్యూటర్లను ఆఫ్ చేస్తోంది**

మార్చవలసిన అవసరం లేదు

ఖచ్చితంగా! భారతదేశంలో సైబర్ చట్టాలు అనే అంశంపై పది బహుళ-ఎంపిక ప్రశ్నలు వాటి సమాధానాలతో పాటు ఇక్కడ ఉన్నాయి:

ప్రశ్న 1:

భారతదేశంలో సైబర్ చట్టాలు ఏమిటి?

ఎ) వ్యక్తిగత ప్రయోజనాల కోసం ఎలక్ట్రానిక్ పరికరాల వినియోగాన్ని నియంత్రించే చట్టాలు

బి) భారతదేశంలో ఇంటర్నెట్ మరియు దాని వినియోగాన్ని నియంత్రించే చట్టాలు

సి) కంప్యూటర్లు లేదా ఎలక్ట్రానిక్ పరికరాలను ఉపయోగించి చేసే భౌతిక నేరాలకు సంబంధించిన చట్టాలు

డి) సైబర్ బెదిరింపు మరియు ఆన్‌లైన్ వేధింపులతో ప్రత్యేకంగా వ్యవహరించే చట్టాలు

జవాబు: బి) భారతదేశంలో ఇంటర్నెట్ మరియు దాని వినియోగాన్ని నియంత్రించే చట్టాలు

ప్రశ్న 3:

సైబర్ చట్టాలకు సంబంధించి భారతదేశంలోని ప్రాథమిక చట్టం ఏమిటి?

ఎ) ఇన్ఫర్మేషన్ టెక్నాలజీ (ఐటి) చట్టం, 2000

బి) ఇండియన్ పీనల్ కోడ్ (IPC)

సి) సమాచార హక్కు (ఆర్‌టిఐ) చట్టం, 2005

డి) వినియోగదారుల రక్షణ చట్టం, 2019

జవాబు: ఎ) ఇన్ఫర్మేషన్ టెక్నాలజీ (ఐటి) చట్టం, 2000

ప్రశ్న 4:

ఇన్ఫర్మేషన్ టెక్నాలజీ (IT) చట్టం, 2000 యొక్క లక్ష్యం ఏమిటి?

ఎ) తపాలా సేవలు మరియు టెలిగ్రామ్‌ల వంటి సాంప్రదాయిక కమ్యూనికేషన్ రూపాలను నియంత్రించడం

బి) విద్యా సంస్థల్లో ఎలక్ట్రానిక్ పరికరాల వినియోగాన్ని నిరోధించడం

సి) ఎలక్ట్రానిక్ లావాదేవీలకు చట్టపరమైన గుర్తింపును అందించడం మరియు ఇ-గవర్నెన్స్‌ను సులభతరం చేయడం

డి) సోషల్ మీడియా ప్లాట్‌ఫారమ్‌ల వినియోగాన్ని నిషేధించడం

జవాబు: సి) ఎలక్ట్రానిక్ లావాదేవీలకు చట్టపరమైన గుర్తింపును అందించడం మరియు ఇ-గవర్నెన్స్‌ను సులభతరం చేయడం

ప్రశ్న 5:

ఇన్ఫర్మేషన్ టెక్నాలజీ (ఐటి) చట్టం, 2000 ప్రకారం "హ్యాకింగ్" నేరం ఏమిటి?

ఎ) కంప్యూటర్ వనరులకు అనధికారిక యాక్సెస్

బి) ఆన్‌లైన్ షాపింగ్ కోసం కంప్యూటర్‌ను ఉపయోగించడం

సి) ఒకరి స్వంత కంప్యూటర్ సిస్టమ్‌ను యాక్సెస్ చేయడం

D) బహుళ గ్రహీతలకు ప్రచార ఇమెయిల్‌లను పంపడం

జవాబు: ఎ) కంప్యూటర్ వనరులకు అనధికారిక యాక్సెస్

ప్రశ్న 6:

ఇన్ఫర్మేషన్ టెక్నాలజీ (IT) చట్టం, 2000లోని సెక్షన్ 66A దేనితో వ్యవహరిస్తుంది?

ఎ) సైబర్ ఉగ్రవాదానికి సంబంధించిన నేరాలు

బి) ఆన్‌లైన్ పరువు నష్టం మరియు వేధింపులకు సంబంధించిన నేరాలు

సి) అనధికారిక యాక్సెస్ మరియు డేటా దొంగతనానికి సంబంధించిన నేరాలు

డి) అభ్యంతరకరమైన కంటెంట్‌ని ఆన్‌లైన్‌లో ప్రచురించడానికి సంబంధించిన నేరాలు

సమాధానం: D) అభ్యంతరకరమైన కంటెంట్‌ని ఆన్‌లైన్‌లో ప్రచురించడానికి సంబంధించిన నేరాలు

ప్రశ్న 7:

ఇన్ఫర్మేషన్ టెక్నాలజీ (IT) చట్టం, 2000లోని సెక్షన్ 66A ప్రకారం మొదటిసారి నేరానికి శిక్ష ఏమిటి?

ఎ) 1 లక్ష రూపాయల వరకు జరిమానా

బి) ఆరు నెలల వరకు జైలు శిక్ష

సి) 5 లక్షల రూపాయల వరకు జరిమానా మరియు మూడు సంవత్సరాల వరకు జైలు శిక్ష

డి) 10,000 రూపాయల వరకు జరిమానా మరియు సమాజ సేవ

జవాబు: సి) 5 లక్షల రూపాయల వరకు జరిమానా మరియు మూడు సంవత్సరాల వరకు జైలు శిక్ష

ప్రశ్న 9:

ఇన్ఫర్మేషన్ టెక్నాలజీ (IT) చట్టం, 2000 ప్రకారం "గుర్తింపు దొంగతనం" నేరం ఏమిటి?

ఎ) సోషల్ మీడియాలో పబ్లిక్ ఫిగర్ వలె నటించడం

బి) మోసం చేయడానికి లేదా అనధికారిక యాక్సెస్ పొందడానికి ఒకరి వ్యక్తిగత సమాచారాన్ని ఉపయోగించడం

సి) వ్యక్తిగత ఉపయోగం కోసం బహుళ ఇమెయిల్ ఖాతాలను సృష్టించడం

డి) అనుమతి లేకుండా ఒకరి Wi-Fi కనెక్షన్‌ని ఉపయోగించడం

జవాబు: బి) మోసం చేయడానికి లేదా అనధికారిక యాక్సెస్ పొందడానికి ఒకరి వ్యక్తిగత సమాచారాన్ని ఉపయోగించడం

ప్రశ్న 10:

ఇన్ఫర్మేషన్ టెక్నాలజీ (IT) చట్టం, 2000 కాకుండా, భారతదేశంలోని ఇతర ఏ చట్టాలు సైబర్ నేరాలను సూచిస్తాయి?

ఎ) భారతదేశంలో సైబర్ క్రైమ్‌లను ప్రత్యేకంగా పరిష్కరించే ఇతర చట్టాలు లేవు

బి) ఇండియన్ పీనల్ కోడ్ (IPC) మరియు ఇండియన్ ఎవిడెన్స్ యాక్ట్

సి) సమాచార హక్కు (RTI) చట్టం, 2005 మరియు వినియోగదారుల రక్షణ చట్టం, 2019

D) కాపీరైట్ చట్టం మరియు పేటెంట్ల చట్టం

జవాబు: బి) ఇండియన్ పీనల్ కోడ్ (IPC) మరియు ఇండియన్ ఎవిడెన్స్ యాక్ట్