నేడు అవలంబించాల్సిన తొమ్మిది ముఖ్యమైన సైబర్ సెక్యూరిటీ అలవాట్లు

1. మీరు క్లిక్ చేయడానికి ముందు పాజ్ చేయండి!

మీకు తెలిసిన వారి నుండి వచ్చినట్లు కనిపించినప్పటికీ లింక్‌లను క్లిక్ చేసే ముందు లేదా అటాచ్‌మెంట్‌లను తెరిచే ముందు ఒకటికి రెండుసార్లు ఆలోచించండి.

- తెలియని లింక్‌లపై క్లిక్ చేయడానికి బదులుగా, ఎల్లప్పుడూ వెబ్‌సైట్‌లను తెలిసిన, చట్టబద్ధమైన మూలం గల వాటి ద్వారా (ఉదా. HTTPS) నావిగేట్ చేయండి.
- అటాచ్‌మెంట్ ఊహించనిదిగా అనిపిస్తే, విశ్వసనీయ పద్ధతి ద్వారా పంపిన వారితో నిర్ధారించండి లేదా సురక్షితంగా ఉండటానికి క్లిక్ చేయకండి.

2. వ్యక్తిగత సమాచారం కోసం అభ్యర్థనలను ధృవీకరించండి

ప్రైవేట్ డేటా కోసం అభ్యర్థనలను ఎల్లప్పుడూ నిర్ధారించండి—అది మీదైనా లేదా వేరొకరిదైనా.

- స్కామర్‌లు విశ్వసనీయ పరిచయస్తుల వలె సులభంగా నటించగలరు.
- అసాధారణ కార్యకలాపాల కోసం ఆర్థిక నివేదికలు మరియు క్రెడిట్ నివేదికలను క్రమం తప్పకుండా సమీక్షించండి.
- అనేక ఫిషింగ్ సందేశాలు అక్షర మరియు వ్యాకరణ దోషాలను కలిగి ఉంటాయి.
- అభ్యర్థన చట్టబద్ధమైనదా కాదా అని పరిగణించండి. వ్యక్తి లేదా సంస్థకు ఆ సమాచారం అవసరమా?

3. మీ పాస్‌వర్డ్‌లను నియంత్రించండి

మీ ఖాతాలను సురక్షితంగా ఉంచుకోవడానికి బలమైన, సంక్లిష్టమైన పాస్‌వర్డ్‌లను సృష్టించడం మరియు వాటిని తెలివిగా నిర్వహించడం చాలా అవసరం.

- విభిన్న ఖాతాల కోసం ప్రత్యేక పాస్‌వర్డ్‌లను ఉపయోగించండి.
- పనికి సంబందించిన మరియు వ్యక్తిగత పాస్‌వర్డ్‌లను వేరుగా ఉంచండి.
- పాస్‌వర్డ్‌లను ఎప్పుడూ షేర్ చేయవద్దు.
- పాస్‌వర్డ్‌ను తరచుగా మార్చండి.
- బ్రౌజర్‌లలో పాస్‌వర్డ్‌లను సేవ్ చేయడాన్ని నిలిపివేయండి.
- అదనపు భద్రత కోసం బహుళ-కారకాల ప్రమాణీకరణ (ఎం.ఎఫ్.ఏ) ని ప్రారంభించండి.

4. మీ పరికరాలను భద్రపరచండి

దూరంగా వెళ్ళేటప్పుడు మీ వర్క్ స్పేస్‌ను లాక్ చేయండి మరియు మీ పరికరాలను రక్షించండి.

- మీ కంప్యూటర్ స్క్రీన్‌ను ఎల్లప్పుడూ లాక్ చేయండి.
- మీ ఫోన్ మరియు పోర్టబుల్ పరికరాలను మీతో తీసుకొనివెళ్ళండి లేదా వాటిని భద్ర పరచండి.
- సాధ్యమైనప్పుడల్లా బలమైన ప్రమాణీకరణ పద్ధతులను ఉపయోగించండి.

5. ముఖ్యమైన ఫైల్‌లను బ్యాకప్ చేయండి

మీ క్లిష్టమైన డేటా క్రమం తప్పకుండా బ్యాకప్ చేయబడిందని నిర్ధారించుకోండి.

- బ్యాకప్‌లను అసలైన వాటి నుండి వేరే ప్రదేశంలో నిల్వ చేయండి.
- సంస్థ ఆమోదించిన నిల్వ పరిష్కారాలను ఉపయోగించండి.
- బ్యాకప్‌లు సరిగ్గా పనిచేస్తున్నాయని నిర్ధారించుకోవడానికి వాటిని క్రమం తప్పకుండా పరీక్షించండి.

6. అనుమానాస్పద కార్యాచరణను రిపోర్ట్ చేయండి

ఏదైనా అనుమానాస్పదంగా అనిపిస్తే, మీ ప్రవృత్తిని విశ్వసించండి- దానిని నివేదించండి!

- మీ సూపర్‌వైజర్‌ని హెచ్చరించండి మరియు అనుమానిత స్కామ్‌లు లేదా అనుమానాస్పద కార్యకలాపాలకు సంబందించి మీ సంస్థ యొక్క రిపోర్టింగ్ ప్రోటోకాల్‌ను అనుసరించండి.

7. మీతో పాటు ఇతరులకు అవగాహన కల్పించండి

తాజా సైబర్ సెక్యూరిటీ బెదిరింపులు మరియు ట్రెండ్‌ల గురించి ఎప్పటికప్పుడు తెలుసుకోండి.

- మీకు అవకాశం వచ్చినప్పుడు శిక్షణా సమావేశాలకు హాజరవ్వండి మరియు సహోద్యోగులతో మీ జ్ఞానాన్ని పంచుకోండి.
- మంచి సమాచారం ఉన్న బృందం సైబర్ బెదిరింపులకు వ్యతిరేకంగా పోరాడడానికి మీ మొదటి శ్రేణి రక్షణ కవచం.

8. సురక్షిత నెట్‌వర్క్‌లను ఉపయోగించండి

ఎల్లప్పుడూ సురక్షిత నెట్‌వర్క్‌లకు కనెక్ట్ అవ్వండి, ముఖ్యంగా సున్నితమైన సమాచారాన్ని యాక్సెస్ చేస్తున్నప్పుడు.

- ఆర్థిక లావాదేవీలు లేదా ముఖ్యమైన పనుల కొరకు పబ్లిక్ Wi-Fi ని నివారించండి.
- అదనపు రక్షణ కోసం అవసరమైనప్పుడు వర్చువల్ ప్రైవేట్ నెట్‌వర్క్ (VPN) ని ఉపయోగించండి.

9. సోషల్ మీడియాతో జాగ్రత్తగా ఉండండి

మీరు ఆన్‌లైన్‌లో షేర్ చేసే వ్యక్తిగత సమాచారాన్ని పరిమితం చేయండి. తద్వారా మీరు మీ గోప్యతను రక్షించుకోవచ్చు, మీ భద్రతను మెరుగుపరచవచ్చు మరియు మరింత సానుకూల ఆన్‌లైన్ అనుభవాన్ని సృష్టించవచ్చు.

- సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లలో గోప్యతా సెట్టింగ్‌లను సమీక్షించండి.
- స్నేహితుని అభ్యర్థనలు మరియు మీ సమాచారానికి పొంద గలుగు వారిని గుర్తుంచుకోండి; లాక్ చేయబడిన ప్రొఫైల్ నుండి అభ్యర్థనలను అంగీకరించవద్దు.
- సంభావ్య ప్రమాదాలను తగ్గించడానికి మీ ఆన్‌లైన్ ఉనికిని క్రమం తప్పకుండా పరీక్షించండి.

గుర్తుంచుకోండి: సైబర్ భద్రత ప్రతి ఒక్కరి బాధ్యత!