ویژه دانشجویان جدیدالورود

توصیه های حفاظتی و فرهنگی ویژه دانشجویان عزیز

دانشجوی گرامی

امام خمینی (رض) می فرماید: دانشگاه کارخانه آدم سازی است. در دانشـگاه بهترین های جامعه جوان کشور جمع می شوند و انتظار می رود بهترین آداب، رسوم و اخلاق در آن رایج گشته تا انسان هایی وارسته، مدیر و مدبر تربیت گردند. خوابگاه های دانشجویی و دانشگاه، خانه دوم دانشجویان محسوب می شود. در این خانه باید همدلی، صفا، صمیمیت، یاری به یکدیگر جاری باشد و از همه مهمتر، امنیت جایگاه بسیار مهمی داشته باشد. چرا که کسـب علم و دانش بدون وجود امنیت عملی نیست. لذا بر ماست برای رسیدن به چنین محیط پویا و با نشاطی تلاش کنیم.

آرزوی ما این است که در دوران تحصیل در دانشگاه برای شما هیچ مشکلی رخ ندهد، اما همان طور که می دانید بسیاری از شکست ها و ناکامی ها به عدم رعایت نکته هایی کوچک برمی گردد. آنچه در ادامه پیش روی شماست بخش کوچکی از شناختی است که بایستی در راه کسب آن تلاش نمایید.

حراست دانشگاه به عنوان مشاور و حافظ امنیت شما در ابعاد مختلف، برای اینکه این مسیر را با سلامت و موفقیت طی نمایید نکاتی را من باب تذکر یادآوری می کند.

بخش اول- توصیه های عمومی :

۱-بزرگترین خطری که امروز جوانان این مرز و بوم را تهدید می کند دام رهایی ناپذیر اعتیاد به انواع مـواد مخـدر و مواد روان گردان است. انـتظار می رود شما عزیزان در این موارد اطلاعات خود را بیشتر نموده تا خدای ناکرده در این دام خانمان سوز گرفتار نشوید و به عنوان یک دانشگاهی، دیگران را نیز نسبت به عواقب شوم آن آگاه نمایید. خوابگاههای دانشجویی باید در شأن دانشجو و دور از مسائل غیر اخلاقی باشد که این موضوع برای اکثر دانشجویان فهیم روشن است اما در عین حال تذکر داده می شود: در صورت عدم رعایت قوانین دانشگاه در خوابگاه، خصوصاً دامن زدن به معضلاتی چون استفاده از انواع مواد مخدر و روان گردان، مشاهده و ترویج فیلم های غیر اخلاقی؛ دانشگاه از طریق کمیته انضباطی جهت حفظ سلامت محیط، با متخلف برخورد جدی قانونی می نماید. چنانچه دانشجویان شاهد تخلفات دوستانشان بوده و سکوت کنند در حقیقت نه تنها به او کمکی نکرده اند بلکه در رسیدن دوستشان به منجلاب های بعدی نیز مقصر هستند، مصداق این مطلب که:

«چو می بینی که نابینا و چاه است اگر خاموش بنشینی گناه است».

۲- مواظب باشید! دعوت های دوستانه خارج از دانشگاه بعضاً به مشکلات حادی مبدل می شوند که بیان آن در این مقال نمی گنجد. تمام فارغ التحصیلان که بیرون از دانشگاه هستند و روزی دانشجو بوده اند افسوس دوران حضور خود در محیط دانشگاه را می خورند. بنابراین همنشینی و رفت و آمد با دوستان خوابگاهی می تواند به نحو شایسته ای زمـینه ارتباط شما را فراهم نمـاید، لذا مواظب باشید تا خدای ناکـرده وارد جریان ناخواسته ای نشوید.

۳- بعضی گروه ها به طور حساب شده، اعتقادات برخی دانشجویان را هدف قرار می دهند. باید مواظب بود و دوست را از دشمن تشخیص داد. شرع مقدس اسلام بر تفکر ، تحقیق و انتخاب راه، سفارش های مؤکد نموده است. در این راستا هرگاه شک یا شبهه ای در ذهن تان در مورد مسائل اعتقادی پیش آمد قبل از این که ذهن شما تحت تأثیر مشورت های انحرافی قرار گیرد

با خبرگان در دسترس یا با کارشناسان محترم نهاد و مرکز مشاوره، وارد سؤال و جواب شوید تا به نتیجه مطلوب برسید. همچنین انس با نماز و مسجد دانشگاه که فضای معنوی آن بی نظیر است؛ می تواند خیلی از دردهای بی درمان حاصل از تنهایی و دوری از خانواده را با معنویت و صفائی که دارد جبران و درمان کند.

۴- از آنجا که امکان سوء استفاده از تلفن های همراه دوربین دار وجود دارد و بـا توجـه به احتمال جا گذاشتن و گم شدن تلفن همراه، توصیه می شود عکس‌های خانوادگی و مسایل شخصی خود را در حافظه تلفن همراه نگهداری نکنید و در صورت استفاده از اینترنت همواره بدانید که مطالب، نوشته ها و مکاتبات شما می‌تواند به راحتی مورد سوء استفاده دیگران قرار گیرد.

۵- خوابگاه یک محیط اجتماعی متشکل از چندین هزار نفر دانشجو می باشد چنانچه در میان هر هزار نفر یک نفر هم با نیت سوء وجود داشته باشد. لازم است شما در حفظ روح، روان و حتی اموال خود از شر بداندیشان بکوشید و علاج واقعه را قبل از وقوع بنمایید.

۶-تقویت و تثبیت آرامش در خوابگاه

- خوابگاه محل زندگی شماست و ضمن دقت در انتخاب هم اتاقی، نمادهای زندگی سالم همراه با آرامش را در آن جاری سازید.
- در صورت مراجعه به منزل فامیل و عدم مراجعه شبانه به خوابگاه، قبلاً مسئولین خوابگاه را مطلع نمایید.
- در صورت بروز هرگونه مشکلی (نظیر اختلاف با هم اتاقی، مشکلات تأسیساتی و ...) مراتب را به مدیریت خوابگاه گزارش نمایید.
- تقسیم کار از مشخصه های زندگی گروهی است لذا جهت جلوگیری از اختلاف و ایجاد فشار روانی، در اتاق تقسیم کار داشته باشید.
- قوانین و مقررات، به منظور رفاه حال شما و تامین نظم تهیه و تدوین شده اند، پس با رعایت هنجارها در بهتر شدن امور به مسئولین کمک نمایید.
- در صورت آوردن وسایلی از قبیل کامپیوتر و ... به خوابگاه مراتب را به اطلاع مسئول خوابگاه رسانده و هنگام خروج نیز با مسئول خوابگاه هماهنگی نمایید تا مشکلی رخ ندهد.
- هر گونه جابجایی اتاق ها، وسایل آن، افراد و...حتماً بایستی با اطلاع مسئول یا سرپرست خوابگاه صورت گیرد.

۷- تقویت امنیت در خوابگاه ها و دانشگاه:

- حتی اگر برای زمان کوتاهی اتاق را ترک می کنید، حتماً درب اتاق را قفل نمایید و کلید اتاق را در مکان های شناخته شده قرار ندهید.
- از رها نمودن کیف و کتاب های درسی خود در کلاس ها و محوطه خوابگاه، کتابخانه، دانشکده یا دانشگاه خودداری کنید.
- برای جلوگیری از هرگونه سوء تفاهم، از اشیاء با ارزش خود مراقبت نمایید و از آوردن اشیای گرانبها و پول بیش از نیاز به خوابگاه خودداری نمایید.
- ترددهای مشکوک را به اطلاع مسئولین برسانید.
- از ورود و دخالت در هرگونه اقدام غیر قانونی از قبیل عدم رعایت شئونات اسلامی، اخلاقی و قوانین، ایجاد مزاحمت، ایجاد رعب و وحشت، درگیری و دعوای بین افراد و هرگونه مواردی که امنیت و سلامت محیط دانشگاه را سلب می نماید، خودداری نموده و مراتب را به اطلاع مسئولین برسانید.

- هرگز فرض نکنید برایتان اتفاقی رخ نمی دهد، پس هم اتاقی یا دوست خود را درجریان اینکه کجا و با چه کسانی بیرون می روید و کی بر می گردید قرار دهید، تا در صورت بروز هر اتفاقی، اقدام به موقع مانع بروز وقایع دردناک گردد.

۸- روش های مقابله با مشکلات:

- تنها خداوند قوی است. به جای اینکه به دامن انسانی ضعیف پناهنده شوید به خدا پناه برید. هیچ کس آنقدر محرم اسرارنیست که تمامی رازها و مشکلات شما را بداند. چه بسا از درد دل های شما سوء استفاده نیز بکند. تنها محرم اسرار خداوند است.
- خانواده مطمئن‌ترین دوست و پشتوانه شماست. در دوراهی‌ها از خانواده حتماً کمک بگیرید، آنها منتظر عملکرد شما هستند و از پیروزی شما خوشنود می شوند.
- حراست دانشگاه متعلق به شماست. هدف آن حفظ امنیت و سلامت روحی و روانی دانشجوست. مشکلات خود را در زمینه های امنیتی با این مدیریت در میان بگذارید تا با استفاده از تجربیات موجود برای رسیدن به هدف یاری شوید.
- جهت رعایت نظم، شئونات و آرامش دانشگاه با انتظامات دانشگاه که در همه مراکز حضور دارند همکاری لازم را بفرمایید و در صورت درخواست کارت دانشجویی شما، با استقبال کارت خود را ارائه نمایید.
- فراموش نکنید در عین حال که بایستی انسانی چند بعدی باشید اولویت اصلی با درس است، پس یاد بگیرید با زمان بندی کارهای روزانه از درس عقب نمانید.
- در مشکلات خود از مشاوره با مراکز ذی صلاح نترسید، از معتمدین خود در مورد کارها و برنامه های درسی خود مشاوره بخواهید.
- به خاطر داشته باشید هیچ گاه برای جبران عقب ماندگی ها دیر نیست. مهم این است که شما تصمیم لازم برای جبران اشتباه را بگیرید.
- برای مصون بودن از شرارت و مزاحمت و جلوگیری از بروز هر گونه مشکلی مسئولین را در جریان مزاحمت ها و حتی تهدیدهای تلفنی قرار دهید.
- اگر از برنامه ها و میهمانی های خصوصی فیلم یا عکس تهیه می شود، به گونه ای حاضر شوید که در صورت هر گونه اتفاق احساس پشیمانی نکنید.
- مراقب باشید قرار دادن اطلاعات خاص علمی، شخصی و خانوادگی روی کامپیوتر متصل به اینترنت پذیرش انتشار آن اطلاعات در سطح وسیع می باشد.
- آنچه شما را در رسیدن به هدف یاری می کند تنها تکیه بر استعدادها نیست بلکه عامل اصلی موفقیت، پشتکار و اراده قوی در مقابله با بروز هر گونه مشکل و اتخاذ تصمیمات درست به خصوص در سال اول ورود به دانشگاه است.
- نسبت به تماسهای تلفنی مشکوک و تخلیه تلفنی حساسیتهای لازم را داشته و مراقب باشید.

بخش دوم – توصیه های حفاظتی در خصوص تخلیه تلفنی :

هوشیار باشید :

- از دادن شماره تلفن های غیرعمومی به افراد ناشناس خود داری کنید.
- هرگونه اطلاعات درون سازمانی که دانستن آن برای عموم جایز نیست، نباید فاش شود.
- برخی اوقات تماس گیرنده، اتفاق مد نظر را به صورتی که مخاطب تحریک شده و اطلاعات بیشتری بدهد تعریف می نماید.
- صرف این که طرف تماس به شما یک شماره داد، دلیل صحت او نیست بلکه باید شماره را بررسی نمایید.

- دادن اطلاعات به تماس گیرنده را به تماس تلفنی خودتان موکول کنید که ضمن اخذ شماره تلفن و چک کردن آن برقرار خواهید کرد.
- آن خاموشی که برای تو سلامت باشد، بهتر از گفتاری است که به دنبالش برایت ملامت باشد.

بخش سوم – توصیه های حفاظتی در زمینه IT :

امروزه امنیت اطلاعات در سیستم های کامپیوتری به عنوان یکی از مسائل مهم مطرح است و می بایست به مقوله امنیت اطلاعات نه به عنوان یک محصول بلکه به عنوان یک فرآیند نگاه گردد. بدون شک اطلاع رسانی در رابطه با تهدیدات، حملات و نحوه برخورد با آنان، دارای جایگاهی خاص در فرآیند ایمن سازی اطلاعات بوده و لازم است همواره نسبت به آخرین اطلاعات موجود در این زمینه خود را بهنگام نمائیم. بدین دلیل و با توجه به اهمیت اطلاع رسانی در این زمینه، به اختصار مطالبی در ارتباط با امنیت اطلاعات، هشدارهای امنیتی، ابزارهای برخورد با حملات و تهدیدات امنیتی تقدیم می گردد.

- **امنیت داده ها در کامپیوترها:**

۱. **عملیات لازم به منظور امنیت داده ها**

- **نصب و نگهداری نرم افزارهای ضد ویروس:**حفاظت کامپیوترهای قابل حمل در مقابل ویروس ها، نظیر حفاظت سایر کامپیوترها بوده و می بایست همواره از بهنگام بودن این نوع برنامه ها، اطمینان حاصل نمود.
- **نصب و نگهداری یک فایروال:**در صورت استفاده از شبکه های متعدد، ضرورت استفاده از فایروال ها مضاعف می گردد. با استفاده از فایروال ها حفاظت لازم و پیشگیری اولیه در خصوص دستیابی به سیستم توسط افراد غیر مجاز انجام خواهد شد.
- **Back up گرفتن داده ها:** از هر نوع داده ارزشمند موجود بر روی یک کامپیوتر باید Back up گرفته و آنها را ذخیره نمود. بدین ترتیب در صورتی که کامپیوتر سرقت و یا با مشکل مواجه شود، امکان دستیابی به اطلاعات در معرض تهدید وجود خواهد داشت .
- **رمزنگاری فایل ها:** با رمزنگاری فایل ها، صرفاً افراد مجاز قادر به دستیابی و مشاهده اطلاعات خواهند بود. در صورتی که افراد غیر مجاز امکان دستیابی به داده ها را پیدا نمایند، قادر به مشاهده اطلاعات نخواهند بود. در زمان رمزنگاری اطلاعات، می بایست تمهیدات لازم در خصوص حفاظت و به خاطر سپردن رمزهای عبور اتخاذ گردد.

۱. **نحوه انتخاب و حفاظت رمزهای عبور:**

رمزهای عبور، روشی به منظور تائید کاربران بوده و تنها حفاظ موجود بین کاربر و اطلاعات موجود بر روی یک کامپیوتر می باشند. مهاجمان با استفاده ازبرنامه های متعدد نرم افزاری، قادر به حدس رمزهای عبور و یا اصطلاحاً " Crack"نمودن آنان می باشند. با انتخاب مناسب رمزهای عبور و نگهداری آنان، امکان حدس آنان مشکل و بالطبع افراد غیر مجاز قادر به دستیابی اطلاعات شخصی شما نخواهند بود. یکی از بهترین روشهای حفاظت از اطلاعات، حصول اطمینان از این موضوع است که صرفاً افراد مجاز قادر به دستیابی به اطلاعات می باشند. فرآیند تأیید هویت و اعتبار کاربران در دنیای مجازی شرایط و ویژگی های خاص خود را داشته و شاید بتوان ادعا کرد که این موضوع به مراتب پیچیده تر از دنیای غیرمجازی است. در صورتی که شما رمزهای عبور را به درستی انتخاب نکرده و یا از آنان به درستی مراقبت ننمائید، قطعاً پتانسیل فوق جایگاه و کارایی واقعی خود را از دست خواهد داد. تعداد زیادی از سیستم ها و سرویس ها صرفاً به دلیل عدم ایمن بودن رمزهای عبور با مشکل مواجه شده و برخی از ویروس ها با حدس و تشخیص رمزهای عبور ضعیف، توانسته اند به اهداف مخرب خود دست یابند.

چگونه یک رمزعبور خوب تعریف کنیم؟

اکثر افراد از رمزهای عبوری استفاده می نمایند که مبتنی بر اطلاعات شخصی آنان است، چراکه بخاطر سپردن این نوع رمزهای عبور برای آنان ساده تر می باشد. بدیهی است به همان نسبت، مهاجمان نیز با سادگی بیشتری قادر به تشخیص و کراک نمودن رمزهای عبور خواهند بود. این نوع رمزهای عبور دارای استعداد لازم برای حملات از نوع "دیکشنری "، می باشند. به منظور تعریف رمزعبور، موارد زیر پیشنهاد می گردد :

- عدم استفاده از رمزهای عبوری که مبتنی بر اطلاعات شخصی هستند زیرا این نوع رمزهای عبور به سادگی حدس و تشخیص داده می شوند.
- عدم استفاده از کلماتی که می توان آنان را در هر دیکشنری و یا زبانی پیدا نمود.

- پیاده سازی یک سیستم و روش خاص به منظور به خاطرسپردن رمزها
- استفاده از حروف بزرگ و کوچک در زمان تعریف رمزعبور
- استفاده از ترکیب حروف ، اعداد و حروف ویژه
- استفاده از رمزهای عبور متفاوت برای سیستم های متفاوت
- نحوه حفاظت رمزهای عبور:

پس از انتخاب یک رمزعبور که امکان حدس و تشخیص آن مشکل است، می بایست تمهیدات لازم در خصوص نگهداری آنان پیش بینی گردد. در این رابطه موارد زیر پیشنهاد می گردد:

- از دادن رمز عبور خود به سایر افراد جداً اجتناب گردد.
- از نوشتن رمز عبور بر روی کاغذ و گذاشتن آن بر روی میز محل کار، نزدیک کامپیوتر و یا چسباندن آن بر روی کامپیوتر، جداً اجتناب گردد. افرادی که امکان دستیابی فیزیکی به محل کار شما را داشته باشند، به راحتی قادر به تشخیص رمز عبور شما خواهند بود.
- هرگز به خواسته افرادی که به بهانه های مختلف از طریق تلفن و یا نامه از شما درخواست رمز عبور را می نمایند، توجه ننمائید.
- در صورتی که مرکز ارائه دهنده خدمات اینترنت شما، انتخاب سیستم تائید (**Authentication**) را برعهده شما گذاشته است، سعی نمائید یکی از گزینه های **Public encryption key Challenge/response** را در مقابل رمزهای عبور ساده، انتخاب نمائید.
- بسیاری از برنامه ها امکان به خاطر سپردن رمزهای عبور را ارائه می نمایند، برخی از این برنامه ها دارای سطوح مناسب امنیتی به منظور حفاظت از اطلاعات نمی باشند. برخی برنامه ها نظیر برنامه های سرویس گیرنده پست الکترونیکی، اطلاعات را به صورت متن (غیررمزشده) در یک فایل بر روی کامپیوتر ذخیره می نمایند. این بدان معنی است که افرادی که به کامپیوتر شما دستیابی دارند، قادر به کشف تمامی رمزهای عبور و دستیابی به اطلاعات شما خواهند بود. بدین دلیل، همواره به خاطر داشته باشید زمانی که از یک کامپیوتر عمومی، استفاده می نمائید، عملیات **log out** را انجام دهید. برخی از برنامه ها از یک مدل رمزنگاری مناسب به منظور حفاظت اطلاعات استفاده می نمایند که ممکن است دارای امکانات ارزشمندی به منظور مدیریت رمزهای عبور باشند .

چند عادت خوب امنیتی:

انسان عصر اطلاعات می بایست در کنار استفاده از فن آوری های متعدد، سعی نماید برخی عادات و حرکات پسندیده را برای خود اصل قرار داده و با تکرار مدوام آنان، امکان و یا بهتر بگوئیم شانس خرابی اطلاعات و یا کامپیوتر را کاهش دهد. دستـیابی به یک کامپیوتر به دو صورت فیزیکی و از راه دور، امکان پذیر می باشد. شما می توانید به سادگی افرادی را که قادر به دستیابی فیزیکی به سیستم شما می باشند را شناسایی نمائید. آیا شناسایی افرادی که قادرند از راه دور به سیستم شما متصل گردند، نیز امری ساده است؟ پاسخ سوال فوق، منفی است و شناسائی افرادی که از راه دور به سیستم شما متصل می شوند، به مراتب مشکل تر خواهد بود. اگر شما کامپیوتر خود را به یک شبکه متصل نموده اید، قطعاً در معرض تهدید و آسیب خواهید بود. استفاده کنندگان کامپیوتر و کاربران شبکه های کامپیوتری (خصوصاً اینترنت)، می توانند با رعایت برخی نکات که می بایست به عادت تبدیل شوند، ضریب مقاومت و ایمنی سیستم خود را افزایش دهند. در ادامه به برخی از این موارد اشاره می گردد :

- **قفل نمودن کامپیوتر زمانی که از آن دور هستیم:** شما با قفل نمودن کامپیوتر خود، عرصه را برای افرادی که با نشستن پشت کامپیوتر شما قصد دستیابی بدون محدودیت به اطلاعات شما را دارند، تنگ خواهید کرد.

قطع ارتباط با اینترنت زمانی که از آن استفاده نمی گردد :پیاده سازی فناوری هائی نظیر DSLومودم های کابلی این امکان رابرای کاربران فراهم نموده است که همواره به اینترنت متصل و اصطلاحاً online باشند. این مزیت دارای چالش های امنیتی خاص خود نیز می باشد. باتوجه به این که شما بطور دائم به شبکه متصل می باشید، مهاجمان و ویروس ها فرصت بیشتری برای یافتن قربانیان خود خواهند داشت. در صورتی که کامپیوتر شما همواره به اینترنت متصل است. می بایست در زمانی که قصد استفاده از اینترنت را ندارید، اتصال خود را غیر فعال نمایید .فرآیند غیرفعال نمودن اتصال به اینترنت به نوع ارتباط ایجاد شده، بستگی دارد. چنانچه اطلاعات شما اهمیت زیادی دارد از اتصال سیستم به اینترنت اجتناب کنید.

بررسی تنظیمات امنیتی :

اکثر نرم افزارها نظیر برنامه های مرورگر و یا پست الکترونیکی، امکانات متنوعی را به منظور پیکربندی سفارشی متناسب با شرایط و خواسته استفاده کنندگان، ارائه می نمایند. در برخی موارد همزمان با فعال نمودن برخی از گزینه ها از یک طرف امکان استفاده از سیستم راحت تر شده و از طرف دیگر ممکن است احتمال آسیب پذیری شما در مقابل حملات، افزایش یابد. در این رابطه لازم است تنظیمات امنیتی موجود در نرم افزار را بررسی نموده و گزینه هائی را انتخاب نمائید که علاوه بر تأمین نیاز شما، آسیب پذیری سیستم شما در مقابل حملات را افزایش ندهد. در صورتی که یک Patch و یا نسخه جدیدی از یک نرم افزار را بر روی سیستم خود نصب می نمائید، ممکن است تغییراتی را در تنظیمات انجام شده اعمال نماید، می بایست بررسی مجدد در خصوص تنظیمات امنیتی را انجام داده تا این اطمینان حاصل گردد که سیستم دارای شرایط مناسب و مقاوم در مقابل تهدیدات است.

از دانلود کردن نرم افزارهای موجود در بازار و نصب کپی نرم افزار ها بر روی سیستم خودداری نمایید

به منظور افزایش مقاومت سیستم در مقابل خرابی و از دست دادن اطلاعات، می بایست به ابعاد دیگری نیز توجه داشت. برخی مواقع تهدید اطلاعات و در معرض آسیب قرار گرفتن آنان از جانب افراد نبوده و این موضوع به عوامل طبیعی و فنی دیگری بستگی دارد. با اینکه روشی برای کنترل و یا پیشگیری قطعی این نوع از حوادث وجود ندارد ولی می توان با رعایت برخی نکات میزان خرابی را کاهش داد.

نتایج بی توجهی به امنیت اطلاعات:

نفوذ به شبکه و دسترسی به اطلاعات طبقه بندی شده

تخریب و دستکاری اطلاعات موجود در سیستم و نرم افزارها

اشغال پهنای باند و اتلاف پهنای باند

سوء استفاده های آموزشی، مالی، اداری و... از طریق نفوذ به سیستم های مربوطه

بخش چهارم – توصیه های امنیتی در کلام بزرگان :

** آن که تو را هشدار داد چون کسی است که تو را مژده داد. حضرت علی (ع)

** سخن در بند توست، تا آن را نگفته باشی، و چون گفتی تو در بند آنی، پس زبانت را نگهدار چنانکه طلا و نقره خود را نگه می داری، زیرا چه بسا سخنی که نعمتی را طرد کند یا نعمتی را جلب کند. حضرت علی (ع)

** ای بسا کلمه ای که از تو نعمتی را بگیرد و ای بسا لفظی که خونی را بریزد. حضرت علی (ع)

** نشانهٔ انسان عاقل این است که هر چه می داند نگوید. حضرت علی (ع)

** بسا سخنی که از حمله مسلحانه کارگرتر است. حضرت علی (ع)

** شیعیان ما کم گوی و گزیده گویند. امام صادق (ع)

** در اداره حکومت تنها شناخت و پذیرفتن آن کافی نیست بلکه باید اسرار را از دسترس دشمن و افراد غیر مجاز خودی محفوظ نگهدارد. امام صادق (ع)

** آنچه نمی دانی مگو، بلکه همه آنچه را می دانی نیز مگو، زیرا خداوند بزرگ بر اعضای بدنت چیزهایی را واجب کرده که از آنها در روز قیامت بر تو حجت آورد. حضرت علی (ع)

** به مجرد احراز خطا و اشتباه از آن برگردید و اقرار به خطا کنید که آن کمال انسانی است. امام خمینی (ره)

** کوچکترین کوتاهی در مراعات اصول امنیتی گناه بزرگ شناخته می شود. امام خمینی (ره)

** یک دستورالعمل سخت و محکم ابلاغ شود که هیچ کس حق ندارد از طریق این وسایل مطلب دارای طبقه بندی را منتقل نماید. مقام معظم رهبری

** حکیمی به فرزندش گفت دو چیز را از من بگیر، اینکه بدون فکر (اندیشیدن) مگوی و بدون تعبیر کاری نکن. شیخ بهایی