Advanced Cyber Solutions, LLC.
5500 Ventnor Lane
Springfield, VA 22151
571 205-6893

Online Crime Prevention

Most organizations allow employees the use of IT resources for limited personal use. Corresponding with your child school during work hours, or visiting social media during lunch time are examples of some organizations permitted use of IT resources. Corporate IT users (employees) sometimes abuse these privileges and in doing so they may put their organizations at risk. According to the Internet Crime Complaint Center (IC3) a governmental agency tracking reports of internet crime in the United States, there are many categories of internet crime, and many of those affect not only the individual, but may become access portals to your organization's critical data.

The IC3 list the following as areas of online crime, but these are not all inclusive.

- Auction Fraud
- Counterfeit Cashier's Check
- Credit Card Fraud
- Debt Elimination
- DHL/UPS
- Employment/Business Opportunities
- Escrow Services Fraud
- Identity Theft
- Internet Extortion
- Investment Fraud
- Lotteries
- Nigerian Letter or "419"
- Phishing/Spoofing
- Ponzi/Pyramid
- Reshipping
- Spam
- Third Party Receiver of Funds

Be cautions when navigating the internet with your organization's resources. Although all of these areas above can impact you with just a point-and-click action with your company's resources, participating in them can put you in harm's way, directly or indirectly. Many sites that provide "services" are only entry points to scam artist or industrial thieves. Your access to these sites are dangerous to you and your employer and could be considered grounds for dismissal from your place of employment.

The following are excerpts from the IC3 Online Crime Prevention. To see them all visit www.ic3.gov/preventiontips.aspx

Employment/Business Opportunities

- Do not give your Social Security number when first interacting with your prospective employer.
- Be wary when replying to unsolicited emails for work-at-home employment.

Advanced Cyber Solutions, LLC.
5500 Ventnor Lane
Springfield, VA 22151
571 205-6893

- Beware when money is required up front for instructions or products.
- Be wary when the job posting claims “no experience necessary.”

Identity Theft

- Ensure websites are secure before submitting a credit card number.
- Be cautious of scams requiring personal information.
- Never give a credit card number over the phone unless you initiate the call.
- Monitor credit statements monthly for any fraudulent activity. Review a copy of your credit report at least once a year.
- Report unauthorized transactions to bank or credit card companies as soon as possible.

Credit Card Fraud

- If purchasing merchandise, ensure it is from a reputable source.
- Do research to ensure the legitimacy of the individual or company.
- Beware of providing credit card information through unsolicited emails.
- Promptly reconcile credit card statements to avoid unauthorized charges.

Phishing/Spoofing

- Avoid filling out forms in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the link to which you are actually directed.
- Research what a company’s official website is instead of “clicking a link” from an unsolicited e-mail.
- Contact the actual business that supposedly sent the e-mail to verify if the e-mail is genuine. Do so via your own research or by using the phone number on the back of the card if the message purports to be from a bank or credit card provider or the statements you receive.

Spam

- Do not open spam. Delete it unread.
- Never respond to spam as this will confirm to the sender that it is a “live” e-mail address.
- Have a primary and secondary e-mail address: one for people you know and one for all other purposes.
- Avoid giving out your e-mail address unless you know how it will be used.
- Never purchase anything advertised through unsolicited e-mail.

Every day the IC3 receives complaints from victims who clicked links in an e-mail or paid up-front fees for a product or service only to be conned out of their hard-earned money. Based on the type of scam, there are a number of things a consumer can do to avoid becoming a victim, for additional information visit IC3 webpage. (www.ic3.gov/preventiontips.aspx).

It is good practice to use extreme caution when using your employers IT resources for personal matters. Be conscious that bad actors in the World Wide Web are on the lookout for unsuspecting victims. Do not become a crime statistic.