

## **Consumer Tips for Safely Banking Online**

### **Never save your password to your desktop.**

Saving your password to your desktop may seem like a timesaver but it allows others to access your personal information without your permission.

### **How personal is your password?**

Avoid using passwords that are relevant to your personal situation. Passwords with your phone number, date of birth, or social security number are often gateways to disaster. Create passwords that contain letters and numbers that cannot be easily attributable to you. Change your password every 60 days or as often as you feel comfortable. Remember: The longer the password the harder it is to break it. Use plenty of upper and lower case letters and numbers too.

### **Don't open email from unknown sources.**

"Phishing" emails are those sent to your email address by cyber criminals who wish to steal your personal information. Be wary of any email that asks for PIN numbers, passwords or your credit card information. These letters are often emblazoned with the real registered logos of legitimate companies that you may already do business with. Links within these "Phishing" letters may take you to fraudulent "Spoof" websites which are designed to fool consumers into trusting the integrity of the website. Most Phishing emails do not even address you by your proper name because they are "blanket" emails sent out en masse to thousands of potential targets.

### **Read between the lines!**

Emails do not have boundaries. You may be the recipient of a fraudulent email from any country in the world. Pay close attention to the finer details of any email that you receive. Are there typographical errors or unusual grammatical mistakes within the letter? Is there a hyperlink in the email that directs you to a website address that also bears noticeable errors in language and grammar? Use extreme caution. Do not input your personal information until you verify the website with your financial institution.

### **Report any suspicious emails and website addresses immediately.**

Most E Commerce websites maintain security departments that deal with Spam, Phishing scam letters and other security breaches. Forward any unusual emails and website addresses to the security departments immediately so that they advise you on how to proceed.

### **"We need you to update your password because of a security compromise"**

Why would a company that already has your password request it from you? Many illegitimate emails are sent daily asking you to update your password because of purported "security compromises" that do not exist. A simple phone call to the organization in question will answer any question that you may have regarding security compromises. Customer service centers are to be considered your ultimate resource when you receive potentially illegal or confusing emails.

### **POP UP Windows.**

Beware of any window that "pops up" during an internet banking session. If the window asks you to access another website or to enter your password then you should beware. "RATS" or Remote Access Trojans can be installed on legitimate websites by computer hackers who want to steal your personal information. Call your financial institution's internet banking customer service immediately to determine the legitimate operation of their website before you honor any request for your personal information.

### **Use the best virus protection and firewall protection that you can afford.**

Virus protection and firewalls provide additional layers of protection that you need to insulate your risk exposure to viruses that can rob your computer hard drive of valuable personal information. Virus protection packages and firewalls can be purchased online or at reputable computer software stores nationwide. Remember that after you install virus protection you will still need to regularly update the software to ensure maximum protection. Most software updates are free once you pay for the annual fee for virus protection software.

**Disconnect from the Internet when not in use.**

Literally "unplugging" the PC and disabling your wireless router may play key elements in protecting your information when the computer is not being used. Dial up connections can be unplugged from the telephone outlet while wireless routing devices can simply be unplugged from their electrical source or "powered down" during periods when the PC is idle.

**Allow your financial institution to contact you using normal channels of communication.**

Make sure that your financial institution has your best possible contact telephone numbers and your current mailing address. If your financial institution wishes to contact you they will more than likely use the telephone followed by an actual paper letter sent to your official address.

**Everyone makes mistakes.**

It is always better to obtain guidance from your financial institution when you suspect that you have inadvertently entered your personal information on a bogus website. Do not delay in contacting your financial institution. There are many resources and solutions available to preserve your piece of mind as well as your financial well being. When in doubt-make the phone call!

-- Provided by Fair Isaac to ATMIA and GASA