Your security is important to us. At Comerica Bank, we want to provide the resources and tools you need to help you prevent Internet fraud, and to educate you about online security.

If you're unfamiliar with any of the computer or Internet terms referred to in this guide, please visit **www.webopedia.com.**

Here are some of the most popular terms:

"Phishing" – an online scam that seeks to steal credit card numbers, account information, Social Security numbers, passwords, and other sensitive information by using fake e-mails, fraudulent Internet addresses, imposter websites, and "pop-ups" to impersonate your financial institution and trick you into disclosing your personal data.

"DNS" – the Domain Name Server (DNS) directs traffic around the Internet. A DNS translates domain names into the numeric Internet Protocol (IP) address that is actually used to route Internet traffic.

"Pharming" – can periodically poison the server, causing it to reroute Internet traffic to a fraudulent website when you attempt to visit a legitimate site.

"Spam" – electronic junk mail or unsolicited e-mail.

"Spoofing" – a technique used to gain unauthorized access to computers whereby the intruder hijacks a target's (legitimate website) Internet address to make it appear that fraudulent e-mails are from a trusted source.

CONSUMER ALERT

Don't fall victim to online scams. Just as you would not share your financial information with a stranger who came knocking at your front door, you should not give out personal information online unless you've initiated the transaction.

Online scams seek to impersonate institutions and trick you into disclosing your personal data, which is then used to obtain money or credit fraudulently.

The Internet's usage is continually growing and provides tremendous conveniences to us all. Along with this growth, however, comes the increased risk in protecting personal information while on the Internet.

Comerica Bank has created this brochure as a helpful guide to protecting you from the online scams that exist today.

Remember: Comerica Bank will never request personal information such as Social Security numbers, account numbers, user IDs, PINs, or passwords via e-mail.

Comerica Bank

Consumers can report online scams to the following agencies in order to track trend information and aid future investigations and prosecutions:

- Federal Trade Commission (FTC): **www.consumer.gov/idtheft**
- Internet Crime Complaint Center (IC3) FBI: **www.ic3.gov**
- Forward fraudulent e-mails to the FTC at: **Spam@uce.gov**

Comerica Bank Customers – if you've responded to fraudulent e-mails, please contact **Comerica's Identity Theft Resources at 877-881-8955** from 8 a.m. to 8 p.m. ET, Monday-Friday. For more helpful information, **visit our Consumer Protection Resource Center at www.comerica.com.**

Please forward suspicious Comerica e-mails to Comerica Bank at **Fraud@infosecalerts.com.**

comerica.com

8710161 8/09

Comerica Bank

INTERNET FRAUD PROTECTION

CONSUMER TIPS TO PREVENT INTERNET FRAUD

- **Make sure you know the person or entity you're giving information to,** whether it's over the Internet, by phone, or fax. Do not provide your personal information unless you have initiated contact.

What to look for:

- **Be suspicious of requests for personal information.** Due to the increase of phishing and other online scams, financial institutions have changed their practices and are unlikely to ask you for personal information in an e-mail. Be especially cautious of "urgent" requests, as "phishers" try to excite or upset customers so they will react immediately.
- **Only do business with Internet companies that use a secure form** to capture private information such as account or credit card numbers. A **secure form** will tell you that the site you are about to view is secure and ask if you wish to proceed.
- **Avoid purchasing products from merchant or auction sites if the deal looks "too good to be true."** If it looks too good to be true, it probably is.

Online protection:

- **Don't click the link.** If you are concerned about the authenticity of a financial institution's e-mail, contact your financial institution directly by phone beforehand. You may also go directly to your institution's site by typing the URL in the browser. If you go directly to the site, check for indicators that the pages are secure, such as a padlock symbol at the bottom of the page and a URL that begins with "https" instead of "http."
- **Change your passwords periodically, using ideas that can't be easily guessed.** For example, do not use names (i.e., your mother's maiden name), familiar numbers (i.e., your birthday), or your Social Security number (SSN).
- **Always log off from your online banking session.** Shut off your computer or disconnect from the Internet when not in use.
- **Check merchant privacy policies** and only shop at those that publish policies you agree with.

Computer security:

- **Some phishing attacks use viruses and/or "Trojan Horses" to install programs called "key loggers" onto your computers.**
- **Ensure your computer(s) are equipped with a security toolkit** to help keep trespassers out. A security toolkit includes anti-virus and virus detection software, personal firewalls, and Adware- and Spyware-blocking software.
- **Update the security toolkit frequently,** and periodically check your firewall settings. Install security patches issued by your software vendor. Update software applications as well as operating systems and browsers, and be sure to patch the entire suite of applications that have the same type of operating system vulnerabilities. A number of Internet Service Providers (ISPs) offer toolbars to help identify fraudulent sites. Consider installing a web browser toolbar to help protect you from known phishing websites. Contact your Internet Service Provider (ISP) to determine which is best for you.
- **If you use a wireless network,** install proper encryption, password protection, and secure firewalls.

Is the website credible?

Nothing is foolproof; however, here are some things you can look for to help determine if a website is legitimate:

- **Verify certificates.** If the certificate was issued by an independent certificate authority, due diligence has been performed on the business. If someone has cloned a site, the site will probably not have a certificate. If the certificate name does not match the website, do not use it and notify the owner of the legitimate site. To verify a website's certificate, right click on the website page, click on Properties and then the Certificates button. A legitimate company's web page will most likely have certificate information available, a spoofed website may not.
- **Grammar and spelling.** Is proper grammar and spelling used on the website and/or e-mail? Most companies take many precautions to be sure their websites appear professional. If you notice spelling and/or grammatical errors, be cautious.
- **E-mail notification.** Be aware if the company routinely communicates with its customers via e-mail. If so, would they ask for personal information? If you are unsure of the answer, never respond to the e-mail; rather, contact the company by other means (phone, in person, going to known website, etc.).

Things you can do offline:

- **Always thoroughly tear or shred personal information,** such as pre-approved credit offers, which may contain account information, Social Security numbers, date of birth, etc.
- **Always protect your account information.** Don't write your personal identification number (PIN) on your ATM or debit card. Don't write your Social Security number and/or credit card number on a check. Secure all IDs and passwords so they can't be used by anyone but you.
- **Monitor your accounts and monthly statements thoroughly,** ensuring that all activity is accurate. If your account statements are late, immediately contact your financial institution(s) to ascertain if and when the statements were mailed. If your institution offers online banking, check your account periodically, rather than waiting for monthly statements. (Reporting fraud as soon as possible helps stop further occurrences of fraud.)
- **When using your ATM, shield the inputting of your PIN from sight by other parties** to protect the information from "shoulder surfers."