STAY SAFE!

CYBERSECURITY CHRONICLES
KNOWING THE SOCIAL LANDSCAPE

SOCIAL ENGINEERING CAN BE DEFINED AS THE "ART OF MANIPULATING PEOPLE SO THEY GIVE UP CONFIDENTIAL INFORMATION." ALSO KNOWN AS HUMAN HACKING, SOCIAL ENGINEERING COMES IN MANY FORMS — AND WITH ITS OWN LANGUAGE — AS THIEVES USE EVERY TRICK IN THEIR BAG TO GET WHAT YOU NEED TO PROTECT THE MOST: YOUR SENSITIVE PERSONAL INFORMATION.

PHISHING

WHEN A CYBERCRIMINAL POSES AS A LEGITIMATE INSTITUTION, *USUALLY VIA EMAIL,* IN AN ATTEMPT TO OBTAIN SENSITIVE PERSONAL INFORMATION.

SMISHING

SIMILAR TO PHISHING BUT *CYBERCRIMINALS USE SMS,* THE TECHNOLOGY BEHIND *TEXT MESSAGING,* TO TRY AND DECEIVE YOU.

SPEAR-PHISHING

ORDINARY PHISHING INVOLVES MALICIOUS EMAILS SENT TO A RANDOM ACCOUNT. SPEAR-PHISHING ARE *TARGETED EMAILS* DESIGNED TO APPEAR AS IF THEY COME FROM SOMEONE THE RECIPIENT KNOWS AND TRUSTS.

VISHING

WHEN SOMEONE PERSUADES A VICTIM TO GIVE OUT PERSONAL INFORMATION OR TRANSFER MONEY *OVER THE PHONE,* THIS IS KNOWN AS VISHING. THE CRIMINAL USUALLY CREATES A SENSE OF URGENCY AND ATTEMPTS TO GAIN TRUST BY KNOWING INFORMATION ABOUT THE VICTIM AND PRETENDING TO BE A TRUSTED SOURCE (SUCH AS A FINANCIAL INSTITUTION).

BAD GUY'S ON THE LINE!

WEBSITE SPOOFING

THE CREATION OF A *SHADOW WEBSITE* THAT IS A NEAR REPLICA OF AN ACTUAL SITE.

LEGITIMATE

FAKE PAGE

RANSOMWARE

A FORM OF MALICIOUS SOFTWARE THAT *TAKES OVER YOUR COMPUTER* AND THREATENS YOU WITH HARM, USUALLY BY DENYING YOU ACCESS TO YOUR OWN DATA. RANSOMWARE WILL LOCK YOUR COMPUTER AND DEMAND PAYMENT IN ORDER TO UNLOCK IT.