CONTENT

SOCIAL ENGINEERING

Social Engineering is a technique used by hackers to manipulate individuals into divulging sensitive information. The consequences of falling prey to a social engineering attack can be devastating. This presentation will teach you how to protect yourself.

WHAT IS SOCIAL ENGINEERING

SOCIAL ENGINEERING IS A FORM OF ATTACK THAT EXPLOITS HUMAN BEHAVIOR RATHER THAN TECHNICAL VULNERABILITIES. BY MANIPULATING PEOPLE, RATHER THAN COMPUTER SYSTEMS, ATTACKERS CAN GAIN ACCESS TO SENSITIVE INFORMATION.

TYPES OF ATTACKS

SHOULDER SURFING

SHOULDER SURFING IS WHEN SOMEONE WATCHES OVER YOUR SHOULDER TO OBTAIN YOUR PASSWORD OR OTHER SENSITIVE INFORMATION.

PHISHING

PHISHING EMAILS ARE DESIGNED TO TRICK THE RECIPIENT INTO HANDING OVER THEIR PERSONAL INFORMATION, SUCH AS USERNAMES, PASSWORDS, OR CREDIT CARD DETAILS.

TAILGATING

TAILGATING INVOLVES AN ATTACKER FOLLOWING AN AUTHORIZED PERSON INTO A RESTRICTED AREA BY BLENDING IN WITH A CROWD.

ALBUS SECURITY

COMMON TACTICS USED BY SOCIAL ENGINEERS

PRETENDING TO BE SOMEONE ELSE

SOCIAL ENGINEERS WILL PRETEND TO BE SOMEONE ELSE IN ORDER TO GAIN ACCESS TO RESTRICTED AREAS OR TRICK USERS INTO PROVIDING SENSITIVE INFORMATION.

CREATING A SENSE OF URGENCY

SOCIAL ENGINEERS OFTEN CREATE A SENSE OF URGENCY TO MAKE USERS ACT IMPULSIVELY AND OVERLOOK WARNING SIGNS.

COMMON TACTICS USED BY SOCIAL ENGINEERS

EXPLOITING HUMAN RELATIONSHIPS

BY POSING AS SOMEONE THE VICTIM KNOWS AND TRUSTS, A SOCIAL ENGINEER CAN OFTEN OBTAIN SENSITIVE INFORMATION.

GAINING TRUST

SOCIAL ENGINEERS CAN GAIN TRUST BY PRETENDING TO BE AN EXPERT OR SOMEONE WITH AUTHORITY, LEADING THE VICTIM TO BELIEVE THEY CAN BE TRUSTED WITH SENSITIVE INFORMATION.

ALBUS SECURITY

PHASES OF A SOCIAL ENGINEERING ATTACK

RECONNAISSANCE

THE ATTACKER COLLECTS INFORMATION ABOUT THE VICTIM AND THEIR ENVIRONMENT.

TARGETING

THE ATTACKER SELECTS THE VICTIM AND IDENTIFIES THE TACTICS THAT WILL BE MOST SUCCESSFUL.

DEVELOPMENT

THE ATTACKER SELECTS THE VICTIM AND IDENTIFIES THE TACTICS THAT WILL BE MOST SUCCESSFUL.

DELIVERY

THE ATTACKER DELIVERS THE ATTACK, OFTEN USING MULTIPLE TACTICS TO INCREASE THE CHANCES OF SUCCESS.

EXPLOITATION

THE ATTACKER GAINS ACCESS TO THE VICTIM'S SENSITIVE INFORMATION, OFTEN USING THIS TO GATHER FURTHER INFORMATION AND CONTINUE THE ATTACK.

EXECUTION

THE ATTACKER USES THE INFORMATION OBTAINED FOR THEIR OWN BENEFIT, SUCH AS STEALING MONEY OR USING THE INFORMATION FOR IDENTITY THEFT.

PREVENTATIVE MEASURES AND BEST PRACTICES TO PROTECT AGAINST SOCIAL ENGINEERING ATTACKS

- USE STRONG AND UNIQUE PASSWORDS FOR ALL ACCOUNTS
- ENABLE TWO-FACTOR AUTHENTICATION WHENEVER POSSIBLE
- BE CAUTIOUS OF UNSOLICITED EMAILS OR PHONE CALLS, AND ALWAYS VERIFY THE IDENTITY OF THE SENDER OR CALLER
- KEEP SOFTWARE UP TO DATE AND INSTALL SECURITY PATCHES AS SOON AS THEY BECOME AVAILABLE
- IMPLEMENT EMPLOYEE TRAINING AND AWARENESS PROGRAMS TO EDUCATE EMPLOYEES ABOUT SOCIAL ENGINEERING TACTICS AND HOW TO IDENTIFY AND AVOID THEM
-

ALBUS SECURITY

THANK YOU

+91 7983001181

INFO@ALBUSSEC.COM

@ALBUSSEC.COM