

Cyber

Voice. Text. Email. Face. Identity Theft. Protect. Prevent. Network. Two-factor authentication. Shred documents. One point four million reports of identity theft in 2020 in US – FTC. Strong passwords. Update software. One hundred twenty-four hours spent by consumers resolving identity theft. IC3 – Internet Crime Complaint. Phishing=unsolicited contacts posing as legitimate to steal. Vishing=phone, voice, mail, VoIP. Smishing=text messaging scam.

Pharming=malicious code on computer to re-direct to fake websites. Spoofing=Disguise email, sender, phone number, URL to appear trusted. Text span to 7726 [spam] Cybercrime as a Service (CaaS) Booter services=direct botnets. DNS attacks. Ransomware attacks. Ten strains of ransomware. Five crypto exchanges account for 82% of ransomware attacks. Ransomware gangs. Emotet=botnet on 1.6 million computers. Attach cybercrime infrastructure. Loss aversion. Authority bias. Urgency bias. Halo effect. Present bias. Availability bias. Optimism bias. Change communication channels. Slow down. Office hacks. Camera systems. HVAC. Fire/life safety systems. Elevators and escalators. Lighting systems. Internet connected machines. WIFI networks. Building management and control systems. AV systems. Parking systems. Zipf's law=humans always expend the least possible effort carrying out tasks.