Secure Remote Access
Easy as A, B, C

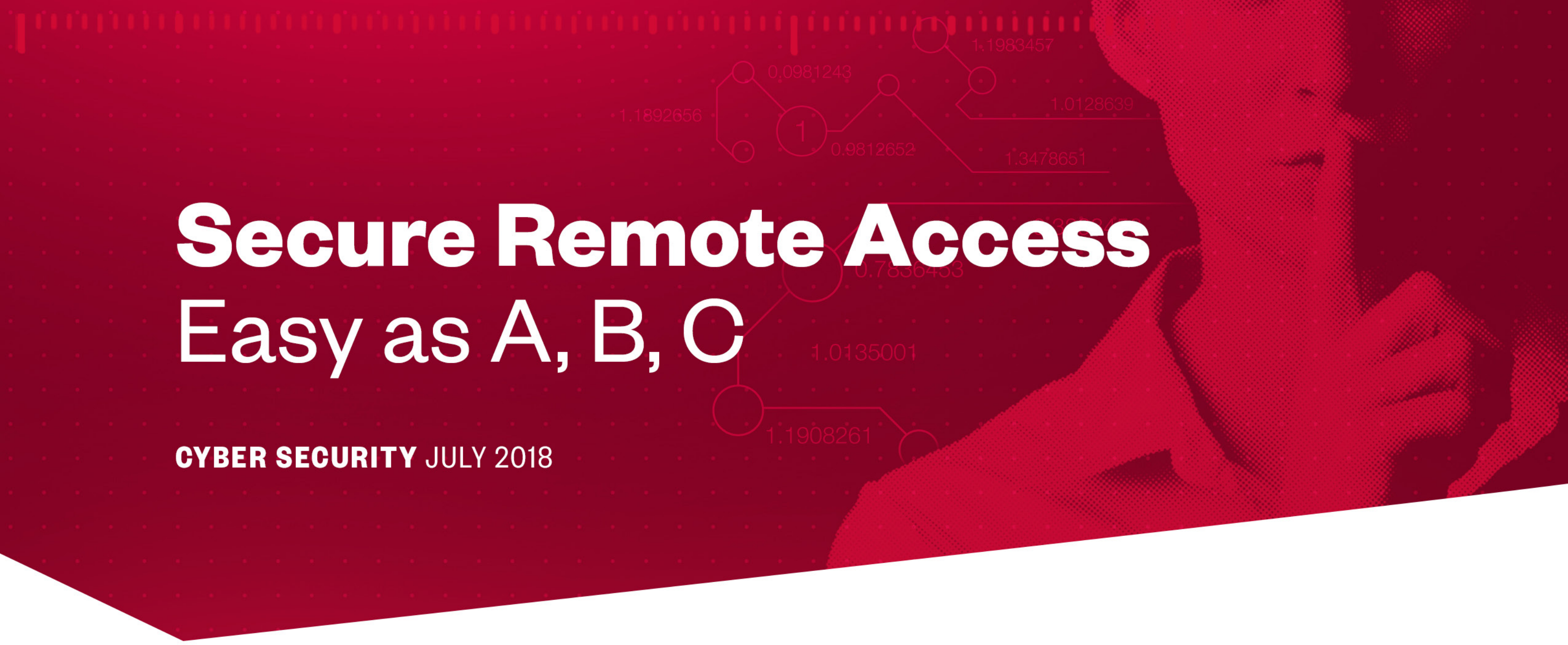
CYBER SECURITY JULY 2018

It is well publicized that today's attackers are ever vigilant in their attempts to uncover weak points in networks, computers, and mobile devices to establish a foothold and leverage vulnerabilities, thus resulting in the compromise of critical assets or personal information. Areas of concern that can lead to a breach include the lack of physical security controls available at remote locations, the use of unsecured networks, and the connection of infected devices to internal networks. The challenge is especially daunting when:

1. Staff, faculty, and students are accustomed to using use free public Wi-Fi hot spots, and some will use them to access institutional e-mails and documents.

2. Some campus employees will e-mail work documents to and from their personal account, despite numerous security problems this creates.

3. Some campus employees will use free USB charging ports available at airports and other public places. These ports pose the risk of transferring viruses and malware to unsuspecting users.



Secure Remote Access
Easy as A, B, C

CYBER SECURITY JULY 2018

Planning for Secure Remote Access

- Assume the worst and plan accordingly
  Laptops and other wireless devices are prone to loss or theft. External networks not controlled by an institution are especially susceptible to compromise and data interception. Finally, remote users' devices may eventually become infected with malware.

- Develop an appropriate remote access policy
  It should define what's allowable in terms of remote access. Data sensitivity is another factor to be considered, as access to confidential or sensitive information should be restricted.

- Configure remote access servers to enforce policies
  Consider the placement of remote access servers at the network perimeter, so it serves as a single point of entry to the network and enforces the security policy before any remote access traffic is permitted into internal networks.

- Employ strong user authentication
  Many external security threats will be mitigated through the deployment of multifactor authentication.

- Ensure personal devices are secured against common threats
  Remote devices should receive the same security applications, software, and devices as those found on campus. They should employ antivirus software and data loss protection capabilities, whenever possible.

- Create a remote access policy
  Users should take every reasonable precaution to ensure their remote access connections are secured from interception, eavesdropping, or misuse. To facilitate this, anyone remotely accessing campus resources for business, maintenance, or upgrade actions should use a virtual private network (VPN) provided by the institution. Also remind staff and faculty not save or store sensitive or restricted institutional data on any remote host or external computing (access) device.

Additional Requirements for System Administrators and End Users

- Apply computer and mobile device security software, applications, and operating system patches and updates regularly.

- Install and use antivirus, antispyware, and VPN software on computers, laptops, and mobile devices, keeping software definitions up-to-date and running regular scans.

- Configure devices so that authentication is required (e.g., password, passphrase, token, or biometric authentication), runs in "least privilege" mode (e.g., user instead of admin), and times out after a 15-minute period of inactivity.

- Activate and use a "lock" feature prior to leaving the computing device unattended.

- Set the security settings to the highest level on Internet browsers and adjust downward as necessary for Internet use.

- At no time should a campus employee provide usernames or passwords to anyone, not even family members.

- Install and enable a hardware and/or software firewall.