IT'S EASY TO STAY SECURE

keep a clean machine

Keep security software current
Having the latest security software, web browser, and operating system is the best defense against online threats.

Automate software updates
Turn on automatic software updates, if available, to defend your machine against known risks.

Protect all devices that connect to the Internet
Smartphones, gaming systems, and other web-enabled devices also need protection from viruses and malware.

own your online presence

Personal information is like money. Value it. Protect it.
Information about you, like your purchase history or location, has value – just like money. Be thoughtful about who gets that information and how it's collected through apps and websites.

Be aware of what's being shared
Set the privacy and security settings on web services and devices to your comfort level for information sharing. It's OK to limit how and with whom you share information.

Share with care
Think before posting about yourself and others online. Consider what a post reveals, who might see it & how it could be perceived now and in the future.

be web wise

Stay current
Keep pace with new ways to stay safe online. Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.

Think before you act
Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.

Back it up
Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely.

connect with care

When in doubt, throw it out
Links in email, social media posts & online ads are one way cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.

Get savvy about Wi-Fi hotspots
Limit the type of business you conduct & adjust the security settings on your device to limit who can access your machine.

Protect your $$
When banking & shopping, be sure the site has security enabled. Look for *https://* or *shttp://*. ***http://* is not secure.**

protect your personal information

Lock down your login
Enable the strongest authentication tools available to protect key accounts like email, banking & social media. Usernames & passwords are not enough.

Unique account, unique password
To help thwart cybercriminals, have separate passwords for every account. Make sure your critical accounts have the strongest passwords.

Write it down and keep it safe
Keep passwords stored in a safe, secure place away from your computer. Or use a password manager to keep track of them.

phishing scams by the numbers

January - September, 2017
Compromised eIDs: 3,555
Phishing Scam Tickets: 5,825
Phishing Scams at K-State: 950

By 2021, cybercrime damage will cost the world $6 trillion annually. (Source: csoonline.com)

The Equifax breach resulted in the exposure of 143 million consumers' personal and financial data.

STOP | THINK | CONNECT

Forward suspected phishing email & original headers to **abuse@ksu.edu**